Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

02-Nov-2004

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Cancels & replaces the same document of 29 October 2004

Task Force on Spam

2nd OECD WORKSHOP ON SPAM

REPORT OF THE WORKSHOP

8-9 September 2004
Busan, Korea

This Unclassified document is a report of the OECD Workshop on spam, hosted by the Korean Ministry of Information and Communication and the Korea Information Security Agency in Busan, Korea on 8-9 September 2004. It is submitted to the upcoming meeting of the Task Force on spam on 22 October for information.

This document will be posted on the OECD Web site on spam at www.oecd.org/sti/spam

Contacts: Christy Bergman; Dimitri Ypsilanti; spam.project@oecd.org

JT00172932

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

2ND OECD WORKSHOP ON SPAM: REPORT OF THE WORKSHOP

The OECD held its 2nd Workshop on spam in Busan, Korea on 8-9 September 2004, which was hosted by the Korean Ministry of Information and Communication and the Korea Information Security Agency. The event attracted some 240 delegates (policy makers, business professionals, researchers and Internet security specialists) representing 24 countries (Australia; Belgium; Canada; Denmark; Finland; France; Germany; Hong Kong, China; Hungary; India; Japan; Korea; Luxembourg; Malaysia; Netherlands; New Zealand; Peru; Singapore; Sweden; Switzerland; Chinese Taipei; Thailand; United Kingdom and the United States).

1. The objective of the workshop was to deepen the results of the first OECD Workshop on Spam, held on 2-3 February 2004 in Brussels, Belgium. At the beginning of the workshop, the OECD announced the formation of an OECD Spam Task Force and presented an outline of its anti-Spam "toolkit" proposal. The remainder of the workshop was dedicated to exploring the framework of the Toolkit and scoping out its Technical Measures element.

2. This document includes a list of main points that emerged from the workshop, followed by summaries of each of the six sessions. It has been prepared by the Secretariat.

3. Presentations delivered at the workshop and other workshop materials are available online via the OECD work on spam Web site at www.oeCD.org/sti/spam

Main points

4. The following key points emerged in presentations and discussions during the workshop and, in particular, reflect the main points highlighted during the last session's moderated discussion on next steps.

Spam is still a problem

5. According to MessageLabs, the average global ratio of spam to desired e-mails was up to 94.5% last July compared to 52.8% last March. Sophos statistics show that this year alone to date, global spam has reached 3 trillion messages with an estimated cost of USD 131 billion and that volumes have doubled compared to this time last year.

6. Not only is the amount of spam up, but also there is increasing propagation of spam across borders and into non-English languages. It is no longer only a problem of OECD economies. For example, ¾ of spam reaching Singapore comes from overseas and about 50% of e-mails to Hong Kong, China ISPs are spam, with 95% of spam in Hong Kong, China coming from overseas including almost 7% from Uruguay and more than 40% from other Asian countries.

7. Phishing attacks are now more numerous, sophisticated and better at fooling victims. Phishing refers to spoofs of a well known institutional (usually a bank or other well-known system such as eBay that handles payments) Web sites that fool the user into divulging private financial data such as account numbers and passwords. Key-loggers can steal passwords and credit card information. Increasingly

organised crime appears to be behind much spam. MessageLabs intercepted 1.7 million phishing e-mails in the first six months of this year compared to practically zero a year ago.

Spam is expected to become a problem on pervasive devices

8. Most young people today use mobile phones more often than computer e-mail, so spam is expected to jump to pervasive devices. However, mass mobile spam is sent via computers to mobile gateways, so controlling e-mail spam is still important for controlling mobile spam. The anti-spam community needs to change the underlying economics of spam and prepare itself for the new technologies. A case in point is that mobile providers, through their commercial contracts to their customers, have practically eliminated the mobile spam problem in Japan and Korea.

Spam and e-mail-born viruses cannot be treated anymore as separate problems

9. Virus writers, spammers and criminals are coming together. Before, the problem of spam was clearly separated from viruses. According to Symantec, two years ago 1/2 000 users carried a virus on their machine, today it is 1/13. The growth rate is linked to spam. Today, the problem of spam cannot be separated from the problem of viruses. The MyDoom virus for example, after an incubation period (time since it was first injected into the Internet until it built a network of zombie drone computers by users who downloaded "worms" attached to spam e-mails) of less than 10 hours, infected more than 350 000 machines worldwide within the next 16 hours (that is only the number of machines cured of the virus by MessageLabs in real-time).

10. A "zombie" computer is a computer containing a hidden software program that enables the machine to be controlled remotely, usually to serve up dubious content and/or send spam without the user's consent and often without the user's knowledge. A user's computer is turned into a zombie when the user installs a spam "trojan" or "e-mail worm". The "trojan" would be installed for example, when the user reads a spam e-mail and sees an innocent-looking filename attached to the e-mail that claims this is a useful program and entices the recipient to open the file. The trojan could also be installed when a user visits a dubious Web site and clicks on a promising-looking icon and then doesn't pay close attention to the pop-up windows asking for verification to install a program. "E-mail worms" are computer programs which can stand-alone and do practically anything, such as sending spam from a user's computer without their knowledge. An e-mail worm, since it is a program, can search the Internet for other computers that have operating system or security holes (e.g. open relays or Windows Authority system shut-down when the RPC system is overwhelmed by denial of service attacks) and install itself on that computer. The very first worms are caught similarly to spam trojans, but become more dangerous over time because of the critical mass they can develop in their install bases.

11. Open relays were called the "oxygen" of spam nowadays. A number of speakers said that we need to cut off the spammer's oxygen supply, that is, eliminate the army of zombies spammers have working for them.

Technical approaches block spam closer to the sender's level

12. The closer spam can be stopped to the sender's level the better. Catching it by filters at the receiver's level is good, but already too late. The burden of spam has already been put on the Internet infrastructure – in the networks and at the receiving e-mail servers of ISPs and organisations. Commercial solutions are beginning to block spam closer toward the sender than the receiver side.

Spammers use multiple techniques, so anti-spam solutions must be multi-levelled

13. Because there are various types of spam, which use various techniques to get at their victims, no single solution to spam can exist. We need to have a diverse and multi-layered arsenal of tools to eliminate spam as well as protect users from spam. Spammers are constantly changing their tactics. The solutions must evolve as well. Legislation alone cannot stop spam as long as it is possible to elude the law by moving operations overseas or hiding one's identity. Technical solutions alone cannot stop spam, as the spammers are constantly one step ahead of the anti-spam community. Self-regulation, co-regulation, and education are also good measures but would not stop spam by themselves. Any solution to spam must thus be multi-layered.

The solution to spam should not be worse than the problem

14. A solution to spam should not make the Internet so cumbersome to use that people stop using it. The cure should not be worse than the disease.

International co-operation is important and not only between governments

15. In the past, when one spoke of international co-operation, one automatically thought of "closed doors" and governmental discussions. Some of the recent trends in international co-operation have been between industries, organisations and the consumer/citizen (Mobile providers and their clients, ISPs, Mailbox providers), and recently between industries and government. Important multi-lateral organisations include the OECD, ITU, APEC, ICANN and ICPEN. International co-operation which is multi-pronged needs to include various different communities in order to be effective.

Authentication is an important technical tool that needs to be developed further

16. Technical authentication does not necessarily mean identification. Technical authentication is not a privacy violation. Technical authentication can serve as a complement to enforcement – supporting the critical evidence necessary to make a conviction. The technical authentication proposals are complementary and any MTA should use multiple authentication methods – in the same way that travellers take several credit cards in their wallet. Care should be taken to balance any technical solution with freedom of information, i.e. the solution should not be so difficult that it stops people from using e-mail.

Education is important, but public trends don't change fast enough

17. Educational campaigns similar to those launched by the U.S. Federal Trade Commission against phishing scams and open relays or by the Japanese MIC against mobile spam, need to be launched against spam trojans or e-mail worms that can turn personal computers into zombies.

18. Education is important, but it is not enough by itself. Even though the public agrees that spam is threatening the Internet and only 8% think the media exaggerates the gravity of spam, the typical end-user is working on a computer that is one year behind in its operating system upgrades and does not have any anti-spam software installed.

The toolkit brings for the first time a multi-pronged approach with global co-operation. For the toolkit to be effective it needs to be broadly based with input not only from OECD governments but more broadly – government, industry, and civil society

19. Cross-border solutions need to be established. Cross-border solutions need to include not only governmental organisations with their national laws but also industry organisations with technical solutions

and industry Memoranda of Understanding. With the speed at which spam is expanding, we cannot wait for the "perfect" solution.

The workshop in Busan was not just a one-off discussion. The work begun in the workshop will be continued by the OECD Task Force on Spam in the form of the OECD toolkit.

Report of the workshop

Welcome and introduction

20. Opening the conference, Vice-Minister Chang-Kon Kim noted that spam was a top priority for the Ministry of Information and Communication (MIC) and a concerted effort to fight spam had reduced the average daily spam in Korea by 43% at the end of last year. Nearly 25% of spam received in Korea comes from abroad. International co-operation was vital to achieve further progress, he said.

21. Mr. Tom Dale, Chair of the OECD Task Force on Spam, said: "While technology is making spamming more difficult, spam is becoming increasingly malicious and damaging to the online environment. Spam is now clearly a tool for significant criminal activity and we aim to assist the development of cross-border enforcement against spammers. The "toolkit" strategy is a fast-track approach to achieve early, and progressive, deliverables." The OECD Spam Task Force will continue this work after the workshop.

Session 1: Developing an anti-spam toolkit

22. This session elaborated on the key elements of an effective anti-spam strategy at the international level beginning with a presentation of the main elements of a proposed OECD anti-spam toolkit. A set of linked deliverables were described including such elements as:

- A spam regulation compendium – a reference to the diversity of existing approaches to spam regulation which will assist policy makers and regulators in making informed choices for the development and the review of regulatory frameworks and arrangements.
- An overview of existing formal and informal arrangements with analysis to help identify what "gaps" may exist and how they might be filled to facilitate the development of international enforcement and cooperative arrangements.
- An examination of the self-regulatory arrangements which exist at industry, national or international levels which can be applied against spam.
- An examination of existing and emerging technical measures against spam, including authentication, and their practical and societal consequences.
- A reference point for education and awareness raising materials that have been developed relating to spam and spam related issues such as phishing.
- An examination of the multi-stakeholder partnerships either in existence or under consideration, including those that could provide useful models for cooperative partnerships against spam.

23. For the toolkit to be effective, it needs to be broadly based with input not only from OECD governments but more broadly – government, industry, and civil society. The fact that there was increasing co-operation across borders was highlighted: such examples include: bi-/tri-lateral co-operation such as: UK-Australia-US MOU on enforcement co-operation, and the Australia-Korea MOU on policy co-operation. Some examples of multi-lateral co-operation include: the OECD Spam Task Force, the

European Union's contact network of spam regulators, ASEM (the Asia-Europe Meeting), APEC (Asia-Pacific Economic Co-operation), UNCTAD (United Nations Conference on Trade and Development), ITU (International Telecommunications Union) and ICPEN (the International Consumer Protection and Enforcement Network).

24. On the economy of spam, the costs are rising (a figure cited was that global spam had an estimated cost of USD 131 billion in 2004 and that volumes have doubled compared to this time last year) meaning that resolving the problem of spam is becoming urgent.. The substantial rise is attributed to trojan infected machines. One major US ISP reports that more than 30% of its users were detected as harbouring remote-access trojans. Phishing attacks have more than doubled this year over last year and the number of detected viruses is up by 21% for the same Jan-June time period. The economic impact of phishing attacks is estimated at USD 222 billion to date (according to the Aberdeen Group Report 2003) with an average profit to the "phisher" of USD5000 per successful transaction. Trojan keyloggers are down to 2 KB in size which makes them harder to detect. An initiative in Australia (www.iia.net.au/spamvt.html) was to develop a spam draft code of practice aimed at the closing of open relays, education of users, law enforcement co-operation and the provision of spam filters.

25. A speaker stressed that although resolving the problem of spam clearly needed a multi-faceted approach, distinct roles could be identified for governments (effective legislation, co-operation on enforcement), industry (self-regulation, technical solutions) and other parties (awareness raising was an area where consumers as well as all other parties had a role to play. In the context of regulation, the European Commission Directive 2002/58 Article 13 Rule 1 sets opt-in permission-based marketing as legal, Rule 2 makes it illegal to hide the identity of the sender and Rule 3 makes the inclusion of a valid return address for opt-out on any direct marketing message a requirement. It also bans e-mail harvesting and misleading advertising. The EC proposes 4 November for a workshop to assess action undertaken since the 2004 EC Communication: (http://www.europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_e.html). In the context of self-regulation, industry (widely defined to include service providers, software vendors, direct marketers, etc.) had a substantial role to play by the adoption of best contractual practices and best marketing practices as well as the development of self-regulatory tools such as codes of conduct.

26. In an overview of spam technical trends, the use of E-mail harvesting spiders that crawl Web pages, dictionary attacks and system hacking to obtain e-mail addresses were described. The blended threat of spam/worm was also described whereby a virus or worm gets onto a user's machine, thereby turning that machine into a "zombie" that can send out spam or serve up dubious content constantly without the user knowing it is happening. It is estimated that 90% of all e-mail worms are spread through spam e-mail with some infamous examples being SASSER 2004, Netsky 2004, Bagel 2004, MyDoom 2004, Blaster 2003, Sobig 2002. Phishing attacks have increased in sophistication – the average lifetime of a phishing site in June 2004 was 2.25 days. That means for detection, it is harder to track them down since the window for verifying the Web site is very short. Anti-spam technical measures were outlined:

- Defensively hiding online e-mail addresses, on personal homepages for example (script conversion of the e-mail, ASCII encryption, hide the e-mail in an image).
- Blocking open relays and open proxies on any TCP/IP connected machine to the Internet, blocking port 25.
- Controlling the granting of e-mail accounts - require a test which verifies a human is behind the request and not just a machine running a script for spammers to create hundreds of dummy e-mail accounts. Examples include hiding a password in an image or requiring the answer to a puzzle before granting the account.
- Rate limiting – setting limits on the number of outbound e-mails and interval between e-mails per day per user.

- Using anti-virus software that can remove a zombie machine from a spammer's zombie network.
- Black/White listing (automatically denying/accepting) e-mail coming from certain domains and/or accounts.
- Filtering e-mails. Filters are heuristic (programmed set of rules behind the filter) or Bayesian (rules are learned by the software using a set of example acceptable/unacceptable e-mails).
- Changing the SMTP e-mail standard to include authentication.
- Increasing the cost of sending e-mails by requiring a monetary fee per e-mail or increased CPU-time per e-mail.

27. In the context of Japan, it was noted that mobile spam to PCs has more than doubled since 2001, but mobile spam, which was initially high, has now trickled down to a small amount, attributable to initiatives by mobile operators in their contracts with their customers. The bulk of Japanese spam comes from Japan. However, due to the rise of phishing attacks, the damage done by mobile spam has increased much more rapidly than that done by phishing attacks to PC e-mail users. Mobile e-mail users tend to be younger than PC e-mail users (60% are under the age of 20). Further analysis shows that mobile spam is unevenly distributed – with young men who use online Japanese dating services receiving the bulk of the total mobile spam in Japan. In response, Japan has launched an educational campaign for students including videos and brochures.

28. The discussion stressed that global co-operation from ISPs is a key requirement to promoting anti-spam solutions. It was also emphasised that anti-spam solutions should go beyond opt-in/opt-out legal discussion and concentrate on making spam illegal under all existing laws. However, care needs to be taken to ensure that the solution to spam is not so burdensome so as to create a disincentive to use e-mail.

29. A question was raised and answered that the OECD would work synergistically with the United Nations International Telecommunications Union, where the most efficient scenario is one where the developments are made in the OECD and the results are spread using the UN as outreach. Regarding whether/when/where the OECD toolkit would be published, different elements of the toolkit will progress at different paces, but the toolkit skeleton overview will be available in the coming months. Self-regulation, and co-regulation will be addressed separately because they mean different things in different countries. The toolkit will provide a broad view and could lead to a path toward possibly an international convention, but that technical solutions will improve more quickly than any regulatory convention.

Session 2: Network management solutions

30. This session discussed a number of different solutions to spam focusing on network solutions. The view was put forward that the SMTP out-bound e-mail server is where spam should be charged. Today ISPs have to make a difficult judgement as to which e-mails are "harmful" and false positives do occur frequently. A speaker described an online stamp system whereby a "white list" allows "stamped" e-mail to pass through without checking, while everything else is DNS-filtered. At the end-user's mailbox, a graphical user interface shows a "stamp" icon next to e-mails from senders in the stamp system and a complaint button and offers a feedback/reward system to users who give opinions on e-mails to the ISP. Interest was expressed in inter-ISP co-operation on a global level to implement a global "stamp" system.

31. Other speakers re-emphasised that it is important to stop spam at the source. Most users have machines that are one year behind in operating system patches and are without anti-spam software. It was argued that most ISPs are not responsive to complaints from other ISPs. This unresponsiveness leads to indiscriminate blocking of port 25 or 254 completely, an over-reaction to what could be more intelligently dealt with if ISPs were to better co-operate on a global scale. It was argued, that many ISPs have outdated ownership records and poorly staffed abuse desks. In addition, the lack of co-ordination between ISPs is exploited by spammers. Because ISPs are not sharing publicly their blacklists, 3rd parties currently offer

this service: RBL (commercial), Spamhaus (free), SORBS, Blackhole (more radical and covers Chinese and Korean language spam). ISPs could cooperate by alerting another ISP if they see a known spammer change ISPs. Best practice for ISPs is that they each provide a Postmaster and Complaint mailbox. It was suggested that ISP administrators use VOIP to keep in touch with each other via the INOC database: http://www.PCh.net/inoc-dba/.

32. In the case of one specific country, Switzerland, today it is possible to base complaints against spammers on the provisions of Swiss data protection law, since e-mail addresses qualify as 'personal data'. Because the Swiss universal service obligation applies to traditional voice telephony only, the Swiss National Regulatory Authority doesn't consider the implementation of Black Lists to be conflicting with the Swiss telecommunications law. In fact, the Swiss government encourages ISPs to make use of all technological means available in order to protect their users, infrastructures and services. The currently ongoing revision of the telecommunications law is expected to clarify the matter by obliging ISPs to fight spam. Concerning mandatory authentication, a speaker said, “The spamming phenomenon demonstrates that market failure in the form of negative externalities is present, which justifies regulation in that area”.

33. Further arguments were made that solutions needed to be applied earlier i.e. at the network and application layers, rather than later when the traffic has already reached the end user. A draft proposal called Identified Internet Mail (IIM) is under consideration by the Message Authentication Signature Standards (MASS) of the Internet Engineering Task Force (IETF), the body that decides on Internet “standards”. In the IIM proposal, the receiver checks a “fingerprint” of the sender’s public key with a Key Registry Service (procedure is like domain registration and the KRA server could be the DNS server) to see if the binding is “good”. In response to critics who say that spammers could spoof the key authentication, a time-to-live is put in the binding of the message with the signature (authentication) and Message Authentication Code (MAC for integrity). Another criticism of authentication systems is that spammers are able to “jump through the hoops” and pass the authentication better than anybody. For example, 34% more spam gets through SenderID authentication than “normal” e-mail because the spammers are typically technologically more knowledgeable than the average Internet user. In IIM, a 3rd party would be responsible for rating senders. This 3rd party aspect would provide market niche opportunities for CA-type organisations which would keep each other competitive. The “rating” could be thought of like a credit rating that stays with an individual sender. Thus, spammers who set up disposable e-mail accounts could not establish a good “rating” because such ratings take time to build.

34. IIM filtering also works for Voice over Internet Telephony (VoIP). IIM as well as Domain Keys, are considered “identity-based” approaches to authentication. ISPs should be given the tools to decide what to do, given the information whether a certain e-mail validates with IIM or not.

35. The question was raised and answered that even if spammers tried to circumvent the TTL in the IIM binding, that they would still be caught by the reputation system time-developed “rating”. A DNS server could be the Key Registry server. Concerning the INOC DB, an IP phone costs USD 70 these days and that since they are owned by ISP administrators, a call on such a phone is the most effective way to take a node down. On the issue that E-postage is restricted by currency, it was pointed out that 1 cent per e-mail may be cheap in developed countries but it is expensive in a country like India. The opinion was voiced that the “stamps” idea was geared toward enterprises and was a way to “buy” a white list”.

Session 3: The role of authentication

36. Authentication schemes fall into two categories. The first category are IP-based (identify the domain of the last-hop or the last Message Transfer Agent). Examples include SenderID and SPF. The second category are crypto-based (identify the original sender at the first-hop). Examples include IIM, Bounce Address Tag Validation (BATV) and Domain Keys. Authentication proposals are complementary

and MTAs (an intermediary stage in the Internet e-mail architecture) should implement multiple authentication schemes. As an example, people usually travel with multiple credit cards in their wallets, in the case that one card won't work. In terms of adoption, IP-based authentication methods are the easiest and crypto-based methods are the hardest. IP-based authentication has already started; crypto-based authentication could start mid-2005.

37. However, in the different authentication proposals, different things are being authenticated. The problem with the current SMTP specification is that the "mail-from" field only tells where to reply/send complaints. It does not tell us who sent the e-mail. Some of the authentication proposals under consideration by the IETF include:

- BATV (under the MASS working group) proposes to add encoding into the "mail-from" field to tell whether it corresponds to the actual sender of the e-mail or not.
- The SMTP HELO is MTA-to-MTA domain authentication, meaning that it determines if the e-mail was authorized at least from the last MTA.
- Client SMTP validation (CSV) proposes to authenticate the SMTP HELO.
- SenderID and SPF verify whether the e-mail client was authorized on behalf of the domain to send e-mail.
- IIM and Domain Keys would authenticate the actual sender of the e-mail.

SPF and SenderID had been merged into a single proposal under consideration by the MARID working group in the IETF (the IETF has since rejected the joint authentication proposal as a possible Internet standard and decided to disband the working group).

38. It is necessary to consider that authentication until now was not in the application layer on either the sending or receiving side in Internet e-mail architecture. In order to be effective, SPF authentication has to be performed at each step in the e-mail bounce path. That is why SPF is sometimes referred to as "path-based" authentication.

39. It should be noted that authentication provides information on "who", but it does not provide information on whether the sender has accreditation (reputation). The best is a multi-layered defence at multiple levels: the message content, message author, message transfer service, traffic analysis. To do this, all message identifiers and content should be authenticated, "reputation" services should be set up and users educated (education alone will not be sufficient since spammers can spoof URLs as well as mail-from fields). When considering the time to implementation, one has to consider that if changes are made to the mail user agent, individual users will have to update/upgrade their e-mail software, which could take time. With the zombie networks, spam now includes millions of machines. Authenticating a single machine or a single user won't be enough. It will have to be done on a massive scale to be effective. The Internet today has over 1 billion users and counting! In considering solutions, we need to be cautious and we should not choose "just one" solution.

40. One easy security measure is to choose a better password (it is recommended to use at least one number, one punctuation mark and mix upper/lower cases in your password to make it harder to guess with a "dictionary attack"). Prices have dropped on many physical security devices: USB keys with random access numbers electronically generated, crypto-keys and biometrics (fingerprint recognition is only USD 100 now).

41. It was predicted that ISPs will start using authentication early in combination with filtering. ISPs would use content signing on the edges of the network for outgoing e-mail. Education will be important to roll this out to consumers. ISPs should get ready with their help desk to help users upgrade their system configurations and e-mail software upgrades. Large domain owners (e.g. ISPs, EBay) will be able to make

the necessary changes sooner than the general public (5-10 years). Technical authentication does not violate privacy and data protection laws because it identifies the e-mail identity, not the real identity. To check if your network is a source of AOL-received spam, you can go to http://postmaster.aol.com/ .

42. It was emphasised that the Internet community must ensure that in using authentication for spam, the costs of implementing authentication be less than the costs imposed by spam. Authentication systems must meet a number of basic objectives: minimum failure rate, be robust, simple, flexible and compatible with legal frameworks. Further, such systems must be open, be easy to use and transparent. There also must be a transition period for implementation and the architecture has to be platform independent.

43. A question on how much consensus is needed for a technical authentication approach to move forward was discussed. Authentication will require a change to the infrastructure, but whether that change is to be made in the interior "network" or the edge "clients" will be part of the answer. Having large ISPs adopt first may be beneficial because that would provide a certain core level of consensus, but care would have to be taken not to overlook the different operational requirements that small ISPs and individuals have which are different from large ISPs and to iron out these functional issues before spreading any authentication solution out to the masses or edges.

44. Another important consideration in this area has to do with the extent to which authentication systems would impact the processing requirements of DNS servers. A number of proposals being put forward, such as SenderID, SPF, IIM and Domain Keys would all require a modification to be made to the DNS record. SenderID would need a new or modified DNS record. SPF would require a small script which could be put into the DNS text record. With Domain Keys, operation and management of the public key would become necessary. DNS servers could become a vulnerable point of attack.

45. In the context of phishing, a long wait for authentication systems to be put in place is not an option problem, Phishing is growing at 50-100% per year. One solution to phishing is use of 3rd-party companies that warn users through toolbars when a site is not authentic. Many large banks compile lists of known sites and warn the public.

Session 4: New technologies and mobile spam, Part 1

46. Spammers profit from the law of large numbers and the economics of spam. One response to half a million spam e-mails is enough for 400 responses per day. A "response" for the spammer is that the receiver makes a phone call, goes to a certain URL or does some specific action. Given that the average profit per transaction is USD 20, a spammer can make USD 8000 per day! And this is just the income for an average spammer. A skilled spammer can make much more.

47. Spammers continue to change their techniques. For example, they may mask URLs using % codes to fool the user. Filters try to keep up with spammers. Filters can be applied at three levels: mailbox, server and network. At the network level, the simplest filter is a white/black list that lets through without checks certain known senders ("white") or blocks outright e-mails from certain known spammers ("black"). Advanced filters use heuristics based on analysis of the message (e.g. if the message contains an over-masked URL). Filters, it is claimed, are working, but the first line of defence against spam is identity (ID + reputation based on history). This is a technical problem that requires a technical solution.

48. Some of the data provided by speakers indicated that in July, 2004 90% of all e-mail to their customers' corporate inboxes was spam. Two years ago 1/2000 users carried a virus on their machine, today it is 1/13. The growth rate is linked to spam. In Asia, the volumes are lower but the trends are the same. There is an increase of spam in different language dialects. E-mail threats besides spam and viruses these days include malware, e-mail worms, spammed trojans, phishing scams, Web bugs and spyware and

denial of service attacks (DoS). There was a 45% increase this year in phishing. There are higher levels of sophistication in phishing attempts: manipulation of graphics, emulating browser icon, etc. The more sophisticated the phishing e-mail, actually the easier it is to track down!

49. Viruses and spam should be viewed as a joint problem. For example, the MyDoom virus, after an incubation period (time since it was first injected into the Internet until it built a network of zombie drone computers by users who downloaded "worms" attached to spam e-mails) of less than 10 hours, infected more than 350,000 machines worldwide within the next 16 hours (that is only the number of machines cured of the virus in real-time by one vendor). Open proxies are traded online and used to send spam, as well as to host everything from paedophile images to DoS zombies and phishing tools. A mercenary DoS zombie can be hired for as little as USD 60 for 6-hours, or USD 2,000 per week. An open proxy is the spammer's air supply.

50. It was argued that legislation is a requirement but not the entire deterrent. Case in point: even with legislation, there as been no trailing off of spam. Similarly, authentication by itself is not a solution. Statistics show that a higher percentage of spam e-mail complies with authentication than regular e-mail. ISP are a key, central actor and must be accountable to filtering messages. Filtering needs to be done at the Internet level. If not, it is like a water service that doesn't purify before delivering to houses.

51. In Singapore one out of three e-mails is spam and 77% of that spam comes from overseas. Surveys show people rank viruses and spam as the number one and number two most important Internet problems respectively. 74% of people surveyed were aware of anti-spam solutions, but only 1/3 of the users actually used them. In June, Singapore united efforts against spam to include government, three major ISPs, the consumer association, technology federation, business federation, and the direct marketing association. More information is available at http://www.antispam.org.sg.

52. Some technical approaches on the e-mail server, destination e-mail server, and end-user e-mail client:

- At the source e-mail server these methods include rate limiting, authentication, payment systems, and blocking port 25 (SMTP). Solutions at the source e-mail server are the most important.
- At the destination e-mail server approaches include rate limiting, reputation systems (black/white lists), and checking heuristics (e.g. if the same e-mail is sent to many different users).
- At the end-user level approaches include rule-based filtering (e.g. all e-mails with the word "viagra" are to be counted as spam), adaptive filtering (e-mail tool learns what is spam and what is not by your classifications as you read your e-mail, based usually on Bayesian statistics), reputation system (e.g. always accept e-mail from people in your address book).

The danger with anti-spam solutions which are too technical is that it could turn the e-mail system into something that no one uses. Spam was around before e-mail and spam will be around after e-mail because of the economics. We need to raise the cost of spam. Some future forms of spam include Wiki spam and SPIT (spam over Internet telephony that is, spam voice over IP).

53. The discussion emphasised the need to provide early warning to consumers of known phishing sites (e.g. blocking them in the toolbar). In conjunction, anti-spam groups should conduct search-and-destroy online. The importance of being more proactive against phishing was raised. From a government perspective, pre-emptive action would be to put in place laws that give punitive damages. It was generally agreed that enforcement should allow for legal action against spammers in much the same way that credit card fraud is pursued across borders.

54. The role of IPv6 was also discussed. Whereas some participants though that this would help move authentication forward, others argued that IPv6 is applied at the infrastructure not the application layer; while spam is a problem on the application layer. "We need to make changes to communication trends, not to the physical communication layer."

55. To the question on reputation systems of "Who polices the policemen?" the view was put that a federated reputation system is an aggregate of various systems, so there would be built-in market/peer checks.

56. To the aside complaint that e-mail is a burden for bosses who receive hundreds or thousand of e-mails per week because employees see e-mail as face-time with the boss, a response was that collaboration tools make a difference. Socialtext.com, a Wiki knowledge management tool for example, can cut down on corporate e-mails by hundreds per day.

Session 4: New technologies and mobile spam, Part 2

57. In the context of zombie computers, it was stated that these are difficult to detect from an ISP level because the volume of network traffic by each infected PC is so low that it does not stand out in network traffic monitoring. As regards mobile spam, if a spam message is sent from a mobile phone to a mobile phone, the spammer can be identified. Thus, most mobile spam comes from computers to the mobile provider's SMTP server. Technical solutions were reiterated such as filtering, blocking, warning the ISP where the spam came from. In the case of mobile providers, it was suggested the default mobile e-mail address should be changed from the mobile phone number to a mix of randomly configured characters.

58. In Korea, mobile spam complaints for a major operator peaked at the end of 2003 and have tapered off since then. A major reason for the decrease in spam was the revision of the companies "Biz-SMS Agreement" which required that other mobile providers or ISPs wanting to send SMS to the company's mobile subscribers have to send their SMS via the company's gateway. This agreement included adoption of an opt-in function, prohibition on late night delivery, notice of call-back number for disagreement and tightened penalties on those who break the agreement. What this did was make all SMS coming into their system via the usual means identifiable and controllable under their business agreement. At the same time, the mobile operator increased their anti-spam services to customers (following up on violations of the agreement) and distributed an "embedded handset" anti-spam filtering software. Korean mobile spam is almost entirely of domestic origin. Now what rests is to take control of the spam which comes directly to their gateways outside the "Biz-SMS Agreement".

59. In Japan mobile spam increased until 2003 and then decreased, while PC spam has continued to increase. In 2002, the Japanese government passed "The law on regulation of transmission of Specified Electronic Mail". This legislation included opt-out, labeling obligations on the part of senders (including the sender's e-mail address and phone number, e-mail address for opt-out and a "commercial" label for commercial e-mails) and increased penalties. It also allowed telecommunication carriers to refuse to transmit messages which contained random, fictitious e-mail addresses. Complaints about mobile spam decreased until around the time this law was passed and then started to increase.

60. Mobile penetration is 90% in Japan; much higher than e-mail usage. Sending messages is cheaper directly from a mobile than from a PC. However, more e-mail is received on mobile devices than on PCs, while more e-mail originates from PCs than from mobiles. In 2003, the Japanese government formed a working group consisting of all Japanese mobile operators, bulk-mailing e-zine groups and the responsible Ministry. This allowed for self-regulation by mobile operators which included such measures as limiting the number of e-mails sent per subscriber and the ability of mobile operators to suspend services to their

customers who violated their subscriber agreement. These measures helped in reducing spam sent from mobile devices almost immediately.

Session 5: Developments in APEC and other non-OECD economies

61. Spam across all the ITU members as a percentage of all e-mails has grown from 8% to 65% between 2001 and 2004. Developing countries are also dealing with the problem of spam. In such countries, spam has an even more dramatic consequence on Internet access because they lack technical, knowledge and financial resources to face it. As developing economies begin to work towards identifying current legislation and regulations that can be used to fight or prosecute spammers they will need to have access to the knowledge and material from developed economies. For developing economies it was important for them to have access to anti-spam legislation and responsible agencies, help them in formulating anti-spam legislation and get them involved in any multi-lateral co-operation against spam. ITU spam activities can be viewed at http://www.itu.int/spam. In March 2004, there was a virtual conference among regulatory authorities (http://www.itu.int/ITU-D/treg/Events/Seminars/Virtualevents/Regulators). In July 2004 there was a WSIS thematic meeting on spam in Geneva (http://www.itu.int/osg/spu/spam/background.html). In December 2004, there will be a GSR (global symposium for regulators) break-out session.

62. In Hong Kong, China a survey of 11 ISPs indicated that about 50% of all e-mails are spam. Statistics for July 2004 indicated that 95% of spam in Hong Kong, China came from overseas. Of the total spam, approximately 40% came from other Asian countries, 32% from the United States and 8% from Uruguay. Although ISPs have implemented anti-spam procedures there is no consensus on the most effective method. Most believe that legislation would help since none of the existing legislative provisions in Hong Kong, China could directly tackle spam. Regulatory initiatives have been taken including an industry self-regulation Anti-Spam Code of Practice, developing better practice guidelines for ISPs and consumers, developing strategies to close open relay mail servers and compile a common blacklist of spammers. Emphasis is also being placed on user education.

63. In Peru, approximately 70% of all e-mails are spam and approximately 80% of that spam is of domestic origin. Peru has implemented UN resolution 55/63 adopted during the 8th Plenary Meeting of its General Assembly in December 2000 which published 10 measures to combat misuse of information technologies. The Peruvian Ministry of Transport and Communications has identified 8 types of cyber crime, but those which are not covered include spam, computer sabotage, viruses, worms and DoS attacks. This year draft legislation was submitted making spam and the selling of CDs with e-mail addresses a crime. The way it was drafted was through provisions for data manipulation/falsification and false e-mail identity.

64. In the context of international co-operation one could differentiate between bilateral government to government co-operation, between private sector groups, government to private sector, and multilateral. An example of a bilateral co-operation was the Memorandum of Understanding (MoU) between the UK and the USA which was later extended to include Australia as well. MoUs are non-binding "good-will" agreements to make "best efforts". An example of a private sector co-operation is ASTA (anti-spam technical alliance) established by six commercial mailbox company founding members (AOL, British Telecom, Comcast, Earthlink, Microsoft and Yahoo!) and the Internet community. ASTA recommends actions and policies for Internet service providers) and e-mail service providers as well as large senders of e-mail including governments, private corporations and online marketing organisations. Other examples of international co-operation in the category include the IETF, International Chamber of Commerce and International Consumer groups. The MoU signed September 2004 in Beijing between e-Bay, AOL, Yahoo!, Microsoft and the Chinese government is an example of government to private sector co-operation. Examples of multilateral co-operation include the OECD, APEC and ITU.

Session 6: Ensuring coherence and follow-up

65. In the Round Table discussion of the Closing Session it was suggested that the top three issues were how to tackle the zombie problem, authentication which was an important technical tool (but evaluation should begin with consumers to make sure the solution would not deter them from using the Internet) and international co-operation among ISPs via MoUs. Furthermore, it was stressed that there needs to be a coordinated anti-spam solution, that we cannot wait for the "perfect" solution, and that all solutions are meant to be additive. Emphasis also had to be placed on consumer education on how to use the Internet safely ("a driver's license for the Internet") and education on how to complain effectively. It was suggested that governments could help by setting up co-ordinated, Web-based cross-border complaint centres and include private groups in their discussions. Companies need to focus on co-operation with the government, self-regulation and technical developments. Consumers support opt-in.

66. To the question whether we could be educating spammers, the consensus was that sharing data and coordinating globally risks to help the potential victims more than the spammers.

Session 6: Closing remarks

67. Mr. Tom Dale, Chair of the Task Force on Spam, closed the workshop by thanking speakers, panellists, moderators, and participants for their active contributions during the workshop and also the Korean Ministry of Information and Communication for hosting the event and KISA in helping organize the event. He highlighted the fact that commercial solutions are attempting to block spam closer to the sender's level and not only with filters. He noted that in considering Internet standards, the cure should not be worse than the disease. We should be careful that we do not make the Internet so cumbersome to use that people stop using it. The workshop had noted the growth in zombies and in this context self-regulation via security best practice and user education was important. The workshop had highlighted the need to enhance international co-operation between the OECD, ITU and APEC. The process of input to the toolkit should be open so that we can hear the voices of all the relevant groups.

68. The Task Force will deliver individual elements of the Toolkit progressively over the next two years. The next steps will be to finalise the outline for the Toolkit, collect data, inform ourselves better on technical solutions, and to co-ordinate with other international agencies.