ENISA anti-spam workshop

27th and 28th November 2007

London, The New Connaught Rooms, United Kingdom

Table of Contents

Protocol

09:30 – 10:10	*Sarah Radicati, Radicati Group, Inc.* **Opening Keynote: Survival tactics – Understanding & Riding the Messaging Tsunami** Email is getting more and more popular. As of 2007, a person receives and sends 142 emails per day. Not only that, email is also evolving; wireless email and other new communication channels like Wikis, social networks and so on rise up. This brings challenges both for network operators and marketers. The former consider spam as second biggest challenge for their network, outnumbered by viruses only. On the other side, marketers see different challenges. They, as biggest concern, have to bypass anti-spam mechanisms; and this also if recipients regularly subscribed to the information before and the information is actually desired. Anti-spam solutions are mostly applied either on the recipient's desktop computer or as server installation. In 2007, less than 10% of the recipients are protected against spam by appliances. The usage of appliances is expected to increase over the next years due to its simplicity and cost-efficiency. Moreover, reputation based systems will help to get better anti-spam mechanisms by analysing traffic patterns, blacklist entries or other criteria. Currently 20% of all mailboxes are protected by reputation systems. This number will increase soon, which allows porting of this data to other kinds of spam (e.g. spam via Instant Messengers or VoIP). Marketers should follow simple rules in order to be compliant with regulations and to satisfy their recipients. A strict double opt-in procedure will help getting interested addressees only. Marketers should also watch out for compliance. Especially the loss of sensitive data and inconsistent replies to customer inquiries should be avoided. More information: http://www.radicati.com
10:10 – 10:40	*Merijn Schik, European Commission, Information Society and Media* **ePrivacy – European Policy Update** End of 2007, the European Commission made a proposal to update the existing telecommunication package of the European Union. Under the proposal the current legislation is streamlined and consumer rights are strengthened. The reform promotes the wireless economy and reinforces national regulators. The European Commission also suggests to create a new European Authority to better support national regulatory authorities (NRAs) in achieving consistent EU best practices and to facilitate the roll-out of pan-European services. An important new part of the updated regulation is a mandatory breach notification for telecommunication network operators. They have to report significant impacts on their networks and services to National Regulation Authorities (NRAs). Compromised personal data must also be reported to consumers. Enhanced privacy and security obligations build a common set of requirements and help to mitigate risks.

	Based on the proposal, the European Regulators Group (ERG) and ENISA will be incorporated into the new authority. It will therefore serve as a centre of expertise and give assistance to the EC and EU member states. The European Council and the European Parliament will discuss the proposed new legislative measures for an estimated period going up to 2009. Then, the Member States will transpose the agreed directives into their national legislation. More information: http://ec.europa.eu/ecomm
10:50 – 11:10	*Pascal Manzano, ENISA* **Results of ENISA's 2007 Study on Security and Anti-Spam Measures** ENISA's survey on providers' security and anti-spam measures in 2007 aimed at getting a better understanding of security measures used by providers and developing best practices. The survey contained 21 multiple choice questions. All in all 30 Internet Service Providers responded to the survey, thereof three providers from the 10 biggest European providers. The results of the survey show that providers see spam as second most important security threat directly after viruses. Distributed Denial of Service (DDoS) took the third place. A trend shows that providers increasingly use ingress and egress filtering to secure their networks, whereas the usage of egress filtering nearly doubled since 2006. This is a very interesting development, demonstrating that providers are investing in the interest of the Internet community as a whole. Although about the half of providers stated that they use either a Business Contingency (BC) plan or a Disaster Recovery (DR) plan, only 25% of them conduct annual tests of these plans. The survey found out that almost every provider offers anti-spam solutions for free, only a small part charges a fee for anti-spam mechanisms. Methods used are mainly blacklisting and content filtering by 82% and 75% of providers, respectively. Greylisting and sender authentication checks are also used by every second provider. However, more than 80% of providers use SMTP authentication methods for outgoing emails. In addition, between a third (Reverse MX) and a half (Sender Policy Framework - SPF) of all providers publish DNS based authentication records. Providers also take outgoing spam into account. About a half of providers limits the outbound email volume and/or blocks access to TCP port 25 from all hosts of their network, in order to mitigate spam caused by botnets. More than 60% of all providers perform outbound virus scanning. If a subscriber continuously sends spam, he is put on a blacklist by 62% of all providers. A small fraction of 10% of providers uses a different approach and use a whitelist for subscribers who do not send spam. When getting complaints about spam which was received from their network, 73% of all providers process these complaints manually. 8% uses the ARF reporting format for automated processing. The rest of providers use another reporting format or automated tool to process complaints. Regarding all technical measures, more than a third of all providers see a

	conflict between the usage of filters and their obligations to secure the network. These issues are covered by the following contribution about legal aspects of Email Screening, presented by Andrej Tomšič. Participants of the workshop asked about the low response. ENISA stated that many providers and provider associations were contacted to participate in the survey. However, only a few of them responded to the survey. ENISA assesses the followed surveying approach and will improve it in the coming year. More information: http://enisa.europa.eu/
11:10 – 11:30	*Andrej Tomšič, Information Commissioner of Republic of Slovenia* **Presentation of Article 29 Working Party Opinion 2/2006 on Email Screening** Providers often see conflicts between filtering anti-spam emails and privacy of users. The opinion 2/2006 of the Article 29 Working Party (WP29) provides guidance on the questions of confidentiality of email communication and, more specifically, on the filtering of on-line communications. A legal framework for privacy protection and privacy in email communications is given in European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) as well as in two European Directives covering data protection (Directive 95/46/EC) and e-Privacy (Directive 2002/58/EC). Based on these, the Opinion 2/2006 deals with screening in emails for detecting viruses, predetermined content in emails and filtering spam. Screening of emails for purpose of detecting viruses might be justified by the providers' obligation to take appropriate measures to safeguard security in their services. However, the content attached to an email must not be disclosed to anyone but the addressee. Even virus-infected annexes must be handled confidentially. Screening of emails for purpose of filtering spam can also be justified by the providers' obligation to perform the service contract properly and therefore securing their network. To avoid conflicts, providers should inform subscribers of their anti-spam policy in a clear and unambiguous way. Since false positives raise conflicts with freedom of speech and constitute an interference of private communications, WP29 recommends giving subscribers the possibility to opt-out of email scanning for filtering purposes. Moreover, providers are strongly recommended to give their subscribers a chance to check emails deemed as spam. Another option can be to provide subscribers with a way to decide what kind of spam should be filtered out. Screening of emails for the purpose of detecting any predetermined content is prohibited without the consent of the user. In exercising such type of filtering, email service providers become censors of private email communication. The Opinion 29 is not seen as legal act itself that should be implemented

	in the law. It depends on the NRA whether and how the opinion is enforced. Not all EU member states implement this opinion directly. However, all member states are bound to the legal framework the opinion is based on. Greylisting is considered as privacy friendly. However, no sending party is informed about greylisting and the delay of delivery for legitimate email senders might be high. ENISA commented that greylisting is an effective method as long as it is not widely used. Sooner or later spammers will adapt to this method, when too many providers implement it. Providers asked whether it is mandatory that a user has an option to opt-out from anti-spam measures. WP29's opinion is that users must be informed in an unambiguous way. Giving them a choice to unsubscribe from email screening avoids legal issues. More information: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm
11:50 – 12:20	*Prof. Rotert, EuroISPA* **The challenge and Opportunities for ISPs in the Fight Against Spam** EuroISPA, a pan-European association of European Internet Service Providers (ISPs) associations, represents the European ISP industry on EU policy and legislative issues. It supports national ISP associations in exchanging best-practice in anti-spam and other ISP related issues, like botnets, filtering or rights of action. EuroISPA gave several reasons why spam should be countered by ISPs. Firstly, it increases network security and stability due to less traffic and virus incidents. Secondly, costs for data processing as well as customer support are decreasing when spam is mitigated. In the end, providers will gain a better reputation when countering spam. If customers receive less spam, they will be more satisfied. Also related providers will acclaim other providers when joining them to combat spam. The European Commission supports EuroISPA in its call for right of action. This will allow ISPs to take legal initiatives to prosecute for concealing an identity. However, private sector enforcement actions might be complementary to those of data protection acts. Therefore, EuroISPA tries to persuade the EC that dissuasive sanctions should also result from private sector enforcement. Members of EuroISPA see conflicts between anti-spam recommendations given by regulators. For example, the EC asks ISPs to implement egress filtering. On the other hand, the European Working Party Article 29 provides guidance on the questions of confidentiality on the filtering of on-line communications. In this matter, false positives (i.e. legitimate traffic that is filtered falsely) are a main concern and might harm data protection acts. Related to this, EuroISPA asks for a clearer statement on non-liability. ISPs can apply incoming and outgoing filters. In the opinion of EuroISPA, blocking on entry basis should not be seen as filtering at all. Under this

	category fall blocks based on RFC non-compliance or IP addresses. If real filtering is applied, providers are uncertain how to filter correctly. For example, putting presumed spam to a separate spam folder or tagging spam emails might interfere with the integrity of email communications. Eventually, outgoing filters are not addressed by the Article 29 Working Party. Recommendations to mitigate especially the botnet problem are given by well-known provider associations (like MAAWG). However, implementation of those might be difficult, since contractual conditions between providers and their subscribers probably need to be changed. Discussion showed that in the end botnets are a big problem. They could be taken into a database of evidence for legal actions against users of infected computers. However, it is hard to distinguish between infected computers and end-users who purposefully send spam. Managing port 25 is a possible solution, which on the other hand might attract spammers to improve their bots to use smart hosts of the providers with stolen user identities. In the worst case, this could jeopardise the integrity of a provider's official email relay. Providers usually do not dare to give additional burdens to their users (e.g. a walled garden). However, making such measures mandatory nationwide (as done e.g. in Sweden) will help to educate users and manage the problem of botnets without having providers loosing customers. A comment from a member of Article 29 Working Party clarified that Article 29 does not require perfect filtering. Article 29 only requires providers to make their filtering transparent and inform or better ask subscribers. Email marketers asked for a dedicated entity they can speak to when having spam related issues. EuroISPA consider themselves as good contact point, but highlighted contacting national provider associations as a good starting point. Related to this, a Certified Senders List was presented during the talk of the German ISP association eco e.V (see below). Some participants wondered whether all providers are able to implement the new framework on network security (as presented by the EC before). EuroISPA mentioned that smaller providers probably will not implement the regulations. However, medium/large providers are expected to adapt their measures to the new framework. More information: http://www.euroispa.org/
12:30 – 13:00	*Anthony Smyth, IronPort* **Stock Spam is on the Rise** IronPort presented some recent spam statistics. They see botnets as a serious problem, leading to massive amounts of spam. An estimation of 98 billions of spam emails per year was mentioned, recognising a steadily increasing tendency. Moreover, taking effective measures against spam becomes difficult. Nowadays already a third of all spam emails are image spam, stressing the networks of ISPs. Other kinds of spam, like phishing, PDF spam, MS Excel spam and even MP3 spam makes the combat difficult. The median

	outbreak time of botnets decreased from 315 to 160 minutes. In other words, the time from infection until first spam sent from a bot is less than three hours. IronPort considers the economics of spam as the original problem. Known incomes of spammers have shown that the criminal ecosystem is real and profitable. Zombies, i.e. participants of botnets, enable the attack by applying sophisticated and extraordinary spam techniques. After a question from the audience, IronPort answered where spam geographically comes from. Spam mostly origins in 3rd world countries or more general, in countries which have anti-spam legislation which lags behind (e.g. Russia, China). IronPort does not see an end of spam. In contrary, whenever email spam will be stopped, spammers will use other techniques to spread their unwanted advertisements (e.g. spam via VoIP or video streams). More information: http://www.senderbase.org
14:00 – 14:30	*Thomas Rickert, eco e.V.* **SpotSpam – Results of the Pilot Phase of the European Spambox Project** SpotSpam is an international database project in order to gather end user complaints about unlawful electronic communication. The project was co-funded under the EC Safer Internet Programme and is now ready to use. Information stored in the database is made available for enforcement and threat assessment purposes. SpotSpam's goal is to face the network abuse problem by improving international co-operation between providers, end-users and legal entities. The general idea of SpotSpam is to set up a centralised database, which is fed by national spamboxes. Such national spamboxes are operated by trustworthy and both private and public parties. Complainants, i.e. end users can send data to this spamboxes, or directly to the database. This is made possible after a registration via a web interface or email forwarding. Data in the database is then used to create analysis reports and clustering campaigns. It is made available either via Data Request Agreements or queries on non-personal and non-confidential data (e.g. IP address of sender, spamvertised URL, etc.) only. SpotSpam helps to show requesting parties contact points of investigators in order to help in a specific case. After finishing a prototype database and the creation first national spamboxes, SpotSpam is looking for participants in the roles of national spamboxes, requesting parties or supporters. Possible benefits are an increased effectiveness of complaints made by end-users and regularly tailor-made reports about incidents. In the end, SpotSpam might help to reduce the workload for the enforcement agencies. More information: http://www.spotspam.net/
14:40 – 15:05	*Prof. Dr. Norbert Pohlmann, Institute for Internet-Security* **IP Reputation Exchange**

Anti-spam mechanisms can operate on different layers. Network level methods like blacklisting are a first check when receiving an email. In general, they are the most efficient way of blocking illegitimate emails. The later anti-spam methods are in the flow of an email, the more resources are needed to process this email. Therefore an improved version of network level is needed – an IP reputation service.

Usually every ISP administrates its own white- and blacklist and spends many resources on doing so. The basic idea of IP reputation services is to exchange these local lists of IP addresses and additional information like dial-up net ranges. Working together with other providers can basically have two positive effects. Firstly, every provider gets new information that they can use easily to enhance their view on the IP address space. Secondly, providers save much time to build up their blacklists, since they gain new information automated via an IP reputation service.

Combining multiple blacklists can increase the effectiveness of blacklists dramatically. The basic idea of a distributed IP reputation service is therefore to connect network participants willing to share IP reputation data, such as black- and whitelists or dialup net ranges. The goal of such a Trusted Peer Network is to get a nearly complete IP map of the entire advertised IP address space.

During the discussion it was stated that a pilot system of the distributed IP reputation service was developed by the Institute for Internet-Security. Although there exist major benefits from this system, fears were mentioned that ISPs might not want to join this system due to legal aspects or the complexity of this system. Marketers mentioned that distribution of reputation also means several contact points in case a listed entity wants to be delisted, making the procedure more complicated than in a centralised blacklist.

More information: https://www.internet-sicherheit.de

15:05 – 15:20

Christian Rossow, Institute for Internet-Security

Improving our Good Old Blacklisting

Blacklisting can be considered as the most important and effective anti-spam solution available for providers. However, there is less information available online, which blacklists a provider should use to combat spam.

A comparison between publicly available blacklists shows intersections between blacklists. These similarities are caused by data exchange among blacklist operators and spammers triggering many sensors when sending a bulk of spam. An intersection matrix shows the actual percentages, to which parts a blacklist is covered by other blacklists. The lower the intersection ratio between two blacklists, the higher is the benefit when combining them.

When providers want to assess blacklists, they basically care about the false positive and false negative rates of those. The latter can be determined by using spamtraps and querying against blacklists. However, false positive rates cannot be measured with this method. An

	implementation of a hamtrap will help to measure false positive rates, by using legitimate emails taken from moderated mailing lists. Mapping blacklisted IP addresses to countries shows that European providers not only have problems with receiving, but also with sending spam. As an example, the blacklist CBL contains many European IP addresses; three out of the worst ten countries are from Europe, which is a warning sign for European ISPs. More information: http://dnsbl.if-is.net
15:30 – 16:00	*Dipl.-Inform. Hadmut Danisch* **Towards a More Secure European Internet** Hadmut Danisch, the inventor of the anti-spam method Reverse MX (RMX), presented his long-term experiences from his engagement against spam. He presented his ideas, recommendations for future approaches and new anti-spam proposes. Spam can be considered as symptom instead of a real problem. The actual problem should be solved in order to cure the spam problem. This requires smart, simple and open approaches. It should be kept in mind that anti-spammers can adapt to new methods. Global anti-spam approaches are likely to fail due to different mentalities, incompatible legal systems and deviating concepts of security. A possible approach for solving not only the spam problem would be letting every network participant decide on its own with whom to communicate. This could be done by three different proposals. Firstly, bits of the IPv6 can be used to specify the provider and country of origin of an IP packet. Secondly, X.509 certificates should have a special european extension identifying the owner of the certificate as a legal entity and under which jurisdiction he resides. Further security extensions for Web browsers are required. Both alternatives offer the option to decide with whom to communicate, e.g. only specific countries etc. As a last possible approach, Mr Danisch suggested to eliminate insecure computers from vital communications by secure programming, access control software and application profiles. Since all aforementioned options are long-term, ad-hoc measures were suggested. A European database cataloguing known software (applications, patches etc.) could help to check communication partners for possible vulnerabilities. Moreover, undocumented hardware and unmaintained proprietary drivers should be prohibited. More information: http://www.danisch.de
Day 1: **16:00 – 16:30**	*Panel headed by Roger Dean; with contribution from Des Fitzpatrick (Office of Fair Trading), Sara Radicati (The Radicati Group Inc.), Skip Fidura (OgilvyOne Worldwide Ltd.), Dr. Vangelis Ouzounis (ENISA), Merijn Schik (European Commission)* **Panel Discussion: SPAM WARS III – EUROPE STRIKES BACK!**

	During the first panel session, the new European legal framework and its implementation by providers was discussed. Merijn Schik, member of the EC, mentioned that the new framework adds proposals to specific topics and does not entirely differ from the old framework. Therefore providers only need to adapt some rules. However, providers that did not implement the old regulation now get additional motivation to implement a newer up-to-date regulation. Mr Ouzounis, from ENISA, supported the idea of the new framework, since every extra measure against spam is a step in the right direction and therefore welcomed. Sara Radicati, CEO of The Radicati Group Inc., wondered whether additional legislation can actually help to fight against spam. Most of the spam origins in countries outside of Europe, where European legislation is only a small burden. Only a small percentage of spammers will be touched by the new European framework and therefore technical anti-spam solutions are required. Merijn Schik added that technologies are needed, but not exclusive. He stated that legislation is necessary to support anti-spam technologies, as done by the opinion on email screening from the Article 29 Working Group. For example, this opinion shows that filtering of spam emails is allowed, since providers are enforced to take measures to secure their network. A listener asked whether European law is even useless, since most spam origins in non-European countries. Merijn Schik argued that legislation will help Europe to stop at least outgoing spam. However, additional legislation in other countries might decrease the spam origin in those. Some people in the audience had the opinion that people actually sending spam do not see legislation as a burden. Vangelis Ouzounis added that the goal of the framework is not only protecting people. On the contrary, it enforces Internet Service Providers to take appropriate security measures against network abuse. An ISP stated that it sees problems in finding the balance between anti-spam and related risks such as false positives. Vangelis Ouzounis, from ENISA, concluded that there is no silver-bullet for solving spam. Many possibilities exist, but spammers are clever enough to catch up with their techniques. The new European legislation on electronic communication is more advanced and less complex than legislations of other countries, thus it makes sense to implement it quickly. An exchange of best practices and additional open exchange of working solutions is considered as best path to combat network abuse.
Day 2: **16:00 – 16:30**	*Panel headed by Vangelis Ouzounis; with contributions from Markus Bautsch (Stiftung Warentest), Prof. Dr. Norbert Pohlmann (Institute for Internet-Security), Andrew Cormack (JANET), Andrej Tomšič (Article 29 Working Party), Thomas Rickert (eco e.V.), Pascal Manzano (ENISA)* **Panel Discussion: How to Balance Anti-Spam Measures & Privacy?** The panel was started by discussing which approach is most promising to combat spam. From the users' perspective, fighting spam is seen as task of the Internet Service Providers. They could, as mentioned by other panel participants, for example use an IP reputation system with an appropriate legal framework. Moreover, managing TCP port 25 to mitigate spam and quarantining infected end-user computers (bots) to solve the problem was mentioned as good approach. The participating representative for a provider in the panel round welcomed the aforementioned attempts and

added that educating users to not react on spam will help. Other members asked for clear and enforced regulation to combat spam.

A comment from the audience was made that managing port 25 would solve many problems without higher burdens. However, this might shift the problem of spam. Spammers using direct connections from dial-up computers may steal authentication data and misuse the providers' MTAs for relaying emails. Although this could be handled via egress filtering, managing port 25 is still not considered as a silver-bullet solution. Blocking port 25 traffic has an effect on the user even for legitimate traffic, and routing of traffic misses transparency for the user. Mail user agents (MUAs) make the situation worse by not setting Email Submission via TCP port 587 as default, but instead using port 25 for submitting messages.

Another participant asked why SPF is not applied more widely. Based on the providers study, ENISA commented that providers are offering authentication information records like SPF but only few use it to filter incoming traffic. However, spammers already adapted; the usage of SPF information is very popular when sending illegitimate emails.

Next the correlation between privacy and email filtering was discussed. Since privacy is an elementary human right, this topic is considered as critical. Legal frameworks are produced by lawyers and anti-spam software produced by computer scientists. A workshop participant commented that better co-operation between both groups is necessary. On the other side, users are usually not aware of the fact that unencrypted emails are open like postcards. Due to this, they have a high trust to their providers and often send sensitive data (e.g. credit card details) via email. Eventually the opinion on Article 29 acts as guideline for providers to combat spam with respect to privacy.

Lastly a participant asked whether spam fighting is still needed, or if it would be better to improve the architecture. Since spam is considered as an actual problem, filtering is necessary. If spam overwhelms email communications, the application email will become less reliable. Moreover, providers are eager to save bandwidth and resources. Subscribers usually are more concerned about false positives than false negatives; providers should implement anti-spam methods with regard to this fact.

Spam in other electronic communication channels than email (like spam via VoIP, video streams etc.) will probably appear in the near future. Providers and other parties should prepare to handle them, although still research has to be done. Combating spam and other network abuse has to continue and progress. Simply redesigning the email protocol SMTP will not solve the problem, but merely its symptoms.

Summary

The workshop was set up in order to bring technical and non-technical anti-spam experts together to give an overview about current situation in the area of anti-spam. Professionals from both sides gave contributions about spam trends, current legal and technical anti-spam issues and newest research results.

Discussions during the workshop made clear that providers are fighting spam, but need support from different areas. In general, support from legal experts is highly appreciated by providers. They often seem to stumble in difficult legal aspects regarding email or virus filtering. This workshop made clear which measures are actually desirable and required by policy makers. Moreover, providers welcomed the efforts from research institutes developing new anti-spam technologies.

All in all, the results of the workshop and ENISA’s upcoming deliverable on provider security measures give a comprehensive overview about current anti-spam best practice. However, during the workshop it raised up that spam should be considered as a symptom of network abuse. Solving spam therefore requires, next to current efforts, also approaches to mitigate net abuse in general. As a consequence, ENISA will concentrate next year on resilience as a main part of its Working Programme 2008 and put forth efforts making network abuse more transparent to legal and technical experts.