Taxonomy and Control Measures of SPAM and SPIM

Kamini (Simi) Bajaj and Josef Pieprzyk

Building E6A, Department of Computing,
Macquarie University, North Ryde, Australia
{kamini.bajaj,josef.pieprzyk}@mq.edu.au

Abstract. In this age of electronic money transactions, the opportunities for electronic crime expanded at the same rate as ever expanding rise of on-line services. With world becoming a global village, crime over the internet transcends no boundaries, borders or jurisdictions. This paper critically examines the available literature on spam, and the control measures available to control spam. This study is followed by the literature overview related to mobility of devices and how the application of mobile technologies as communication medium has impacted the handling of spam. The conclusion of this literature review with proposed direction of study is summarized.

Keywords: Spam; Wireless Spam; SPIM; Spam control techniques; Spam Taxonomy.

1 Introduction

With the increase of use of internet, email has become the most popular means of communication. It has gained a lot of popularity as being a very convenient and cost effective means of exchanging messages. The message size in an email may vary from one kilo byte to many megabytes and sending it is very cheap. One of the features of the SMTP protocol is that it allows sending messages to anyone. Consequently, it is easy to send unsolicited email to thousands to recipients with a minimal cost.

1.1 Definition of Spam and Its Impact

The email system may not only be used to circulate messages but also to distribute advertisements in the form of graphics or pictures. The email addresses on the web pages are collected and the virus is appended to emails which then attacks user's personal computers(PCs) for acquiring information [1]. The email addresses are collected in such a way that they are useful for advertisers. However, such emails are called unsolicited emails and hence Spam.

The Word 'SPAM' was originally the brand name for Hormel Foods, maker of the canned "Shoulder Pork and hAM"/"SPiced hAM" luncheon meat. However the term "spam" has today come to mean network abuse, particularly junk E-mail and massive junk postings to USENET. By tracing the history, SPAM originated in 1970's as a

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 529–542, 2012.

repetitive advertising message that was sent to large number of recipients with or without subscribing for the advertising message. SPAM in early 1980's was an innovative way of sending information to large groups of people, however since the last decade it has become a menace.

Spamming is economically viable as the only cost associated is the cost to manage the mailing list [1]. On-line technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity, or to make use of someone else's identity. As a result, even if the user replies to a spam email with disguised identity, it never reaches the sender as the sender address is only temporary.

Recent statistics indicate an increasing problem with spam. The spam numbers have been growing to 45%, 64%, 80%, 92%, 95% for the years 2003, 2004, 2006, 2009 and 2010, respectively ([3,4,5,6,7,8,9]). The most affected countries (with 55% of the total world spam contents) are India, Brazil, Russia, Ukraine, Romania, South Korea, Vietnam, United States, Kazakhstan, Indonesia, Poland, China, Colombia, Israel and Taiwan. The report by MacAfee reveals that in 2008 alone, there were 62 Trillion spam messages sent. They clog the users' inboxes making very difficult to tell apart important messages from spam. They also consume computing and networking resources and are frequently used as a tool for cybercrime activities such as denial of service attack (DoS), distribution of malware, phishing, to name a few.

The abuse of email into spam is done in various ways for example, turning a machine into a relay for spam, a staging ground to attack other systems, or a spy capturing your bank account and credit card information--or all three [2]. According to Ferris Research, the cost of spam mail to organizations in United States was USD 8.9 billion in 2002 with a 12% increase in 2003 to $10 billion and $17 billion in 2005 [3]. They also estimated 40 trillion spam messages sent in 2008, costing businesses more than $140 billion worldwide -- a significant increase from the 18 trillion sent in 2006 and the 30 trillion in 2007 majorly due to employee productivity loss. In Japan, the amount of GDP loss was about 500 billion yen in 2004 [4]. In a press release in 2009, Gartner[1] stated that more than 5 billion US consumers lost money in phishing (type of spam) attacks which was 39.8% more than the year before[5].

1.2 Impact of SPAM (email)

The impact of spam can be shown as:

1. Waste of computing resources - spam consumes bandwidth, introduces delays in routing and unnecessary processing. Some businesses store spam messages to analyze and find a solution.
2. Loss of productivity of users - clearing mail boxes from unwanted email consumes time and can be very frustrating for the recipients.[3]
3. Denial of service - flooding the network with spam can block or create a bottleneck making communication via network impossible [6]

[1] http://www.gartner.com/it/page.jsp?id=936913

4. Invasion of Privacy - collection of email addresses is done without the knowledge of users resulting in the invasion of user's privacy where users receive messages which they do not want to receive.
5. Fraud and Deception - popular kind of spam leading user to a perception of get rich quick schemes for e.g. Nigerian Letter scam. Another case of fraud scam is to lead the user to provide with their confidential access information to their email account or bank details.

2 SPAM in Mobile Devices

The problem of Spam in mobile devices is twofold. While the problem of spam may not bother users so much as on a networked PC, it really affects them on small mobile devices for the reasons of cost, time consumption and inconvenience. If they receive up to 15 spam mails via GPRS or UMTS it does cost real money deleting and getting rid of it on small screen devices. Apart from the usual unsolicited spam messages in inbox, mobile devices also receiving unwanted, unsolicited Instant messages (SMS and MMS). Such Spam in mobile devices is called SPIM (Spam thru Instant Messages). According to report from Adaptive Mobile [7], survey done on smart phone (mobile device) users in UK (1000 participants) in May 2011 reported that 69% received SMS text phishing and 66% SMS spam. In Europe and Asian countries SMS spam is a fashion generating almost half of the total SMS traffic in some countries [8]. The number has been increasing since then [9] reaching 15-25 messages per day . This practice is more common in Asian countries due to poverty and it is easier to lure people to carry out tasks with a lure to make money.

The conversion rate of spam sent compared to products bought is of prime importance in driving the need to reduce spam in mobile devices [10]. Since users of smart phones expose themselves to security risks as reported in [7], 50% would open an SMS text message from someone they don't know, 36% would open an email on their mobile from someone they don't know and 32% save log-in information such as passwords to their mobile, it is crucial to address the problem of spam in mobile devices.

Current mobile devices are offering variety of features for the users such as sending receiving text messages, buying, emailing and many more. Some of the services using these features of mobile devices to carry out their business activities are courier services, Truck GPS systems, and pathology GPS systems. Though these features seem very convenient and useful, attackers are able to take advantage of them [11]. In 2004, Paris Hiltons smart phone was hacked twice and the hackers posted online, intimate photos and personal emails and her address book details causing great deal of embarrassment to all involved [12]. Since 2009 mobile malware threat has been increasing and reports from McAfee labs state that this threat is going to increase even more in 2011 and 2012[13].

2.1 SMS Characteristics

The size of the SMS is generally shorter than the email messages. A typical standard SMS text message contains only 160 characters. It is sent wirelessly using the SMS standard. The user has to open the message to see if it is spam or not since there is no subject. There is a frequent use of abbreviations and acronyms due to the smaller size of the text. The abbreviations and acronyms are not standard for a language; they are dependent upon the user communities such as different age brackets, language, and cultural background. This variability provides sparse representation and variety of features and terms. SMS is a convenient way of communicating when the network or device is busy or unavailable.

2.2 SPIM Characteristics

SMS has become an important medium for mobile advertising due to the nature of use of the device and location specific information availability. Spim has a variety of difference to regular email spam or/and normal message [8, 14-17] .

- Frequent use of abbreviations and acronyms
- Cost per SMS is significant
- Shorter in size, less information to work with
- Community specific varying nature of terms and features
- Additional fields such as attachments, links and images are not commonly used
- The use of topical terms such as ‘buy, free, sale, etc’ cannot be generalized to identify spim as some of these terms could be included in legitimate SMS
- Transmission mechanism- SMS messages are sent either my mobile device or via email. Mobile originated SMS message go from the device to the SMSC and then it may be directed to the other service provider via mobile, fixed or email network. Email originated SMS messages go to SMS gateway first, which then transmits it to the SMSC for delivery to the receiver. Depending upon the location of the receivers device, the SMS is transmitted to the serving SMSC for that location for delivery.

Spimmers clog mobile devices by sending tones of unwanted SMS or MMS and hence making the devices useless. By using text messaging or email, an attacker

could lure user to a malicious site or convince them to install malicious code on your portable device [18]. In any phishing (type of spam- identity theft) attack first few hours are very crucial as many attacks are blocked or the site are taken down after that. The chances that a mobile device user will be hit are much higher than a desktop user, since these spam emails arrive on the mobile users device first and they are 3 times more likely to submit their login details than the desktop users [19].

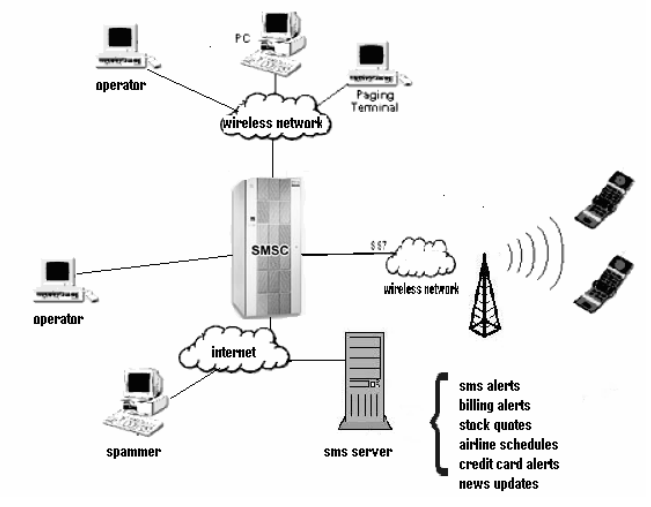

Fig. 1. SMS Network Architecture

The mobile device users receive spam for the three main reasons[17]:

1. Service providers being paid by the third parties to deliver SMS to the user. The providers have an opt out option for the user.
2. Service providers are not aware or paid for the delivery of the SMS to the user. This is a case of fraud as the third parties may use techniques such as online messaging services to send SMS to the user.
3. Users sending the messages to other users (forwarded messages, promotions) with the involvement of service provider.

2.3 Impact of SPAM and SPIM in Mobile Devices

The impact of spam and spim in mobile devices as follows:

1. Abuse of service - Most cell phone plans limit the number of text messages you can send and receive. If an attacker spams the device with text messages, you may be charged additional fees. An attacker may also be able to infect your phone or PDA with malicious code that will allow them to use your service. Because the contract is in your name, you will be responsible for the charges.

2. Luring to a malicious web site - While PDAs and cell phones that give you access to email are targets for standard phishing attacks, attackers are now sending text messages to cell phones. These messages, supposedly from a legitimate company, may try to convince you to visit a malicious site by claiming that there is a problem with your account or stating that you have been subscribed to a service. Once you visit the site, you may be lured into providing personal information or downloading a malicious file.
3. Use of device in an attack - Attackers who can gain control of your service may use your cell phone or PDA to attack others. Not only does this hide the real attacker's identity, it allows the attacker to increase the number of targets.
4. Gain access to account information - In some areas, cell phones is becoming capable of performing certain transactions (from paying for parking or groceries to conducting larger financial transactions). An attacker who can gain access to a phone that is used for these types of transactions may be able to discover your account information and use or sell it.
5. Clogging the device – Once they get access to your device they would send you numerous messages which will clog the device and hence the device will not be able to carry out the service it is intended to do.

3 Taxonomy of Spam

In this section we investigate various categories of spam. Most of these categories are applicable to Networked PCs as well as mobile devices. Many researchers have studied the content of spam messages for developing taxonomies [20-28]. This section focuses on categorizing the content of spam.

Two major Categories of Spam (email as well as SMS and MMS):

3.1 Spam without Attachment

Spam without attachment are mostly text messages with or without clickable URL to a website. Hence can be categorized as:

Content Spam[29]

The content spam contains text messages as means of advertising or scam. For example the Nigerian letters scam. Most of the sender's mail accounts are fake or don't exist. Such emails are limited in number as compared to other categories. In case of text messaging spam in mobile devices as SMS, the spammers target users with lucrative offers and ask them to reply this is at a very high cost.

Link Spam[29, 30]

Contemporary search engines rank web pages by taking into consideration the number of links connected to the pages. A web page to which more links (called in-links) are connected is more likely to be ranked higher. Spammers, therefore, often attempt to manipulate links on the web, for example, add thousands or even millions of links to

the pages which they want to promote – a technique referred to as 'link spam'[30]. On mobile devices, link spam on the messages demands the user to click on a link which would take them to another website to complete the task and hence, either generate numerous amounts on the device and clogging the device for its intended use or compromise identity and details.

3.2 Spam with Attachment

This kind of spam contains combination of image, text and URL or a clickable link to a website. The attachments in most of the cases are image files or executable files. The image files are mostly in .gif format.

Image Spam
Image spam is growing and serious problem. The origin of image spam comes from the conventional spam blocking tools relying on the textual analysis of incoming messages which does not work well against image spam. The volumes of image spam has increased dramatically from <4% in 2005 to over 40% in 2007. In a March 200,7 survey conducted by Osterman Research, more than 60% of messaging decision makers cited image spam as a problem for their organizations. There are various combinations of image spam: Image and text as attachment, Image, text and URL and Image and URL [31, 32].

Image spam on mobile device takes the form of MMS. MMS initially introduced as a mean of sharing pictures with family and friends have taken an abusive form where spammers' send numerous MMS and clogs the mobile device.

Executable file (Virus Spam)[33]
The spam with executable file as an attachment are intended to spread virus, trying to establish mail bombs to plan DDoS attack on the mail server and the network. Upon execution of the attachment, the machine acts as a zombie and performs tasks intended by the spammer such as downloading big programs to harm the network, automatic generation of emails to other in the same domain clogging the entire network. [32]

4 Existing Control Measures

4.1 Regulatory Laws and Legislation

Many efforts have been put in by individuals and organizations such as governments, ISPs, anti-spam organizations, consumer protection organizations, organizations providing anti-spam solution at commercial as well as noncommercial end. An article published by Organization for Economic Co-operation and Development, France provides a list of 39 national and international anti-spam organizations where most of them being noncommercial [34].These measures have been set up by a large number of countries and are basically two kinds of approaches – a. existing laws and

regulations which though not specifically addressed to spam, may nevertheless be implicated by some aspect of spam, e.g. laws to protect consumers from deceptive marketing or to prevent the distribution of pornographic images and b. amendment of existing laws and regulations or new regulations to address the problem of spam are created. There are various kinds of regulatory approaches such as opt-in, opt-out, ISP rights and responsibilities, scope of spam(for example CAN_SPAM for wireless phones and Mobile Devices), spam ware, disclosure of personal data, EU member states and National Cyber Alert systems and complaint mechanisms. 80% of spam in Europe and North America originates from fewer than 200 spammers operating illegally [35].

The laws and legislation addressing mobile devices are: General guidelines provided by US-CERT for mobile devices such as securing your device, posting your device number and email address carefully, not to follow links sent in email or text messages, careful of downloadable software and applying security settings which is also applicable to networked PCs [18]. US Federal Government‘s CAN SPAM Act for mobile devices prohibit sending unwanted commercial email messages to wireless devices without prior permission. The Commission found that Short Message Service messages transmitted solely to phone numbers (as opposed to those sent to addresses with references to Internet domains) are not covered by these protections.

Unfortunately, a code of conduct provides only limited protection against “bad” spammers. Spammers easily find methods to avert systems and/or punitive self-regulatory action, e.g. creative use of programming, switching ISPs, falsifying their identities, etc.

4.2 Education and Awareness

Educating spam victims may have an important impact on reducing spam. Awareness could turn those victims who unknowingly post their email addresses on public sites into spam free users. This also would increase the efforts spammers have to put to collect email addresses. Such social approaches cannot eliminate spam however in general increase awareness about spam and how to deal with it. Legal provisions can control the problem to some extent however steps taken by informed user will certainly help reduce the problem if not eliminate. Consumer protection and government organizations have raised public awareness by informing consumers about spamming tactics and providing them with suggestions on how to prevent spam. Examples are National Cyber Alert System by United States Computer Emergency Readiness team published a document on Defending Cell Phones and PDAs Against Attack [18]. The US Federal Trade Commission operates a Web site dedicated to spam awareness.

4.3 Technical Approaches

List Based Techniques

White-lists (set of email addresses of users whose messages are allowed) and blacklists (email or IP addresses known to be used spammers) are used to filter spam

by using the e-mail address, IP address and DNS address. Real-time Blacklist is one kind of application based on this method. [36] Lists are vulnerable to address spoofing and may also include receiving legitimate messages from users who are not in a white list or who are present in a black list by mistake[37].

Digital Signatures

Digital signatures, also known as fingerprints, identify messages. In some cases where secure data is involved, messages without digital signatures are identified as spam. Signatures of messages that have been identified as spam can be put in a database. This database is then used to compare the signature of received e-mail with the list of signatures of spam. If there is a match, the e-mail is spam [38] [39]. For messages coming through an unsecured channel having a digital signature makes the recipient believe that the message was sent by a claimed sender. The signature can be provided by the sender or the service provider.

Spam Filtering Techniques

Collaborative Filtering

Some organizations prefer tagging/identifying large number of messages sent as spam. They are either labeled as spam and sent to inbox or sent to spam mail box.

Content Based Filtering

Spam filtering is performed at 2 levels mail server level and users email program level. This is post acceptance system. Emails are first received before any filtering is performed. Spam filtering is implemented at various classification methods, all using the features of spam email for classification. The techniques have been classified as content, statistical, rule-based, machine learning and many more.

The techniques are Neural Network Algorithm [31, 39],Boosting, Bayesian Statistics [31, 39], Heuristic[40] [39], Signature based analysis, k-Nearest Neighbor, Decision Trees, Support Vector machines [30, 40], Visualization, Instance based Learning (Ming, Yunchun et al. 2007) [39], Ontology based Machine Learning Approach [41], [42] present a Markov Random Field model based approach to filter spam. This approach examines the importance of the neighborhood relationship (MRF cliques) among words in an email message for the purpose of spam classification.[43] propose a multi-agent based collaborative peer-to-peer system to combine content based filter into p2p collaborative filter, in this way, system can response to new spam rapidly as well as take advantage of the spam knowledge learnt before.

Other Techniques Suggested

Another economic solution suggested is where senders have to pay for emails. [35] This kind of spam control is based on increasing cost to spammers, proportional to the volume of email sent [35, 44].

Several methods have been proposed to detect spam email but the volume of those email continue to grow [45] [21]. This imparts a need for further refinement in the approach used for spam control.

The false positives and false negatives are still great problems, especially the false positives. Generally speaking, misclassifying a legitimate mail as spam is much more severe than letting a spam message pass the filter [36].

5 Mobile Devices Are Not Same as PCs

At present legislation has appeared to have very little effect on spam volumes, some argument suggest that it has increased spam by giving bulk advertisers permission to send spam [46].

In general, mobile devices are not the same as networked personal computers.

- There are many differences between mobile devices and personal computers, and it would be a mistake to consider devices as just smaller versions of PCs. In order to deliver rich experiences onto devices, solution architects need to consider a number of constraining factors, much more so than when delivering applications to a personal computer. These constraints include hardware capabilities of the devices themselves, device operating systems and application runtimes, development tools, connectivity choices, and also available services running on the Web[47].
- With increasing connection capabilities such as 3G/4G voice and data network access, Wi-Fi/WLAN, Bluetooth, WiMax, and UpnP, mobile computing has become more pervasive and ad-hoc than ever [48]. Nodes in a wireless network have limited resources compared to the average wired workstation making spam a serious threat and not just a nuisance [49].
- Mobile devices often use a public transmission medium for (wireless) communication, which implies that the physical signal is easily accessible to eavesdroppers and hackers. Wireless security is a challenging problem, perhaps even more so than wired security in many respects that must be addressed by many mobile devices [50].
- The security of mobile device is different as compared to networked personal computers. Although much has been done to secure networks and devices, a different set of technologies are needed to broker trust among applications running on those devices (and services that they connect to)—technologies for federated identity. These technologies help the user manage multiple digital identities and control how much personal information is shared with other devices and services [47].
- Management of devices does differ in some crucial respects because devices are often much harder to secure: Mobile devices are easy to misplace, and in many cases, access to the devices cannot be restricted [47].

6 Discussion on Control Measures for PCs Verses Mobile Devices

Spam (or spim) on mobile device can be very annoying and inconvenient. Whether it is Blackberry, PDA or Smartphone, it is very frustrating by the lack of built in features to filter spam. There is no software currently available to filter all the spam in mobile devices, although some wireless companies are beginning to place spam filters on their networks to prosecute spammers [35].

Spam Verses SPIM

Although spam and spim have a lot in common there are significant differences between them. Spim like spam mainly consists of commercial advertisements. However, we need to face the fact that spim does not have the same structure and characteristics as spam. Most of the anti-spam techniques are not suitable for spim filtering with accuracy because of the differences in their underlying technology and system infrastructure as well [9]. The characteristics of spim listed in this paper are another major contributing factor among several issues in applying the spam control techniques for wired devices (PCs, wired computers, networks) to mobile devices[8, 14-17]. There would be certain restriction which are as [47]:

- Changes to schema to support mobile extension — there is often little that can be done (or should be done) to change the schema to support mobile applications.
- Data access directly from the database, and update into the tables from the mobile device — often there are several layers of communication to go through and it is not possible to access the database directly from the device.
- Understanding the schema of the data store — schemas for these types of applications are designed to be extended, and as a result can be large and unwieldy.
- Designing a staging area with a schema structure similar to the back end for data to flow to the mobile devices — creating a replica environment for development and staging can be a challenge.

Various authors have suggested techniques to minimize spam in mobile devices [51-54] such as Legal actions, Blacklisting and white listing of the originator, Time- and quota control, limit number of SMS/time interval and per SMSC, Content analysis and filtering, recognition of repetitive text patterns, user data header analysis, block , feature engineering- bag of words, Originating SMSC address prefixes filtering, guards faking, Originator control, IMSI & MSISDN analysis , Challenge response , Blocking the SMS originating from the online SMS generating tools, advanced location analysis, last known location is compared with the calling party, Destination control, IMSI analysis, possible to define different blocking criteria based on the SMS Source and IMSI masking. While a lot of research has happened in the areas of spam control techniques and mobile device/technology, there appears to be dearth of literature and study on the applicability of the control techniques to mobile devices as evident by the statistics of growing amount of losses occurring by obile spam.

This could be attributed to non-applicability of existing spam control techniques to the mobile devices without modifications.

7 Conclusion

It has been 25 years since the first virus was written and since then the security of the devices have been compromised one way or the other, no end seems to be visible [2]. At present Spam and Spim is taking on to become a major problem in mobile devices and before it takes to the heights of spam in networked PCs, this has to be nipped in the bud. The problem of spam in networked PCs is still tacked at some level but the one at mobile devices is a major open issue to be addressed for several reasons: cost, time and inconvenience. Current literature and knowledge shows that security of mobile device is different as compared to networked personal computers.

This research will further investigate into the possibility of adapting the technology in the existing techniques to develop a methodology to minimize spam in mobile devices.

References

1. Takumi, I., et al.: A classification method for spam e-mail by Self-Organizing Map and automatically defined groups. In: IEEE International Conference on Systems, Man and Cybernetics, ISIC (2007)
2. Ford, R., Spattord, E.H.: Happy Birthday, Dear Viruses. Science 317(5835), 210–211 (2007)
3. Ferris_Research Spam Control: The Current Landscape (2007)
4. Takemura, T., Ebara, H.: Spam Mail Reduces Economic Effects. In: Second International Conference on the Digital Society 2008, pp. 20–24. IEEE Computer Society Press, Sainte Luce (2008)
5. Gartner: Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008, 2009 Press Release (April 14, 2009)
6. Nagamalai, D., Dhinakaran, C., Lee, J.K.: Multi Layer Approach to Defend DDoS Attacks Caused by Spam. In: International Conference on Multimedia and Ubiquitous Engineering, MUE 2007 (2007)
7. AdaptiveMobile, Mobile Trust and Security Barometer. Global Security Insight Center (2011)
8. Dixit, S., Gupta, S., Ravishankar, C.V.: LOHIT: An Online Detection & Control System for Cellular SMS Spam. In: Proceedings of the IASTED International Conference, Communication, Network, and Information Security, ACTA Press, Phoenix (2005)
9. Zhijun, L., et al.: Detecting and filtering instant messaging spam - a global and personalized approach. In: 1st IEEE ICNP Workshop on Secure Network Protocols, NPSec (2005)
10. AdaptiveMobile, Global Security Insight for Mobile. Global Security Insight Center (2011)
11. Naraine, R.: iPhone passcode lock bypass vulnerability (again). Security News and Blog (2010)

12. Hong, J.I.: Minimizing security risks in ubicomp systems. Computer 38(12), 118–119 (2005)
13. Security, I.: Mobile Malware on the Rise. News (2011)
14. Yoon, J.W., Kim, H., Huh, J.H.: Hybrid spam filtering for mobile communication. Computers and Security 29(4), 446–459 (2010)
15. De, P.: SMSAssassin - Crowdsourced SMS Spam Filter. Mobile News (2011)
16. Cormack, G.V., et al.: Spam filtering for short messages, Lisboa (2007)
17. Hidalgo, J.M.G., et al.: Content based SMS spam filtering. In: Proceedings of the 2006 ACM Symposium on Document Engineering, pp. 107–114. ACM, Amsterdam (2006)
18. McDowell, M.: Defending Cell Phones and PDAs Against Attack. a.g.o. US-CERT, National Cyber Alert System, USA (2006)
19. Ashford, W.: Mobile users most vulnerable to phishing attacks, study shows. In: IT Management-Security Alerts-News 2011 (2011); Computer Weekly: online
20. Aradhye, H.B., Myers, G.K., Herson, J.A.: Image analysis for efficient categorization of image-based spam e-mail. In: Proceedings of Eighth International Conference on Document Analysis and Recognition (2005)
21. Balakumar, M., Vaidehi, V.: Ontology based classification and categorization of email. In: International Conference on Signal Processing, Communications and Networking, ICSCN 2008 (2008)
22. Chao, X., Yiming, Z.: Transductive Support Vector Machine for Personal Inboxes Spam Categorization. In: International Conference on Computational Intelligence and Security Workshops, CISW 2007 (2007)
23. Chih-Chin, L., Ming-Chi, T.: An empirical performance comparison of machine learning methods for spam e-mail categorization. In: Fourth International Conference on Hybrid Intelligent Systems, HIS 2004 (2004)
24. Drucker, H., Donghui, W., Vapnik, V.N.: Support vector machines for spam categorization. IEEE Transactions on Neural Networks 10(5), 1048–1054 (1999)
25. Islam, M.R., Wanlei, Z., Chowdhury, M.U.: Email Categorization Using (2+1)-Tier Classification Algorithms. In: Seventh IEEE/ACIS International Conference on Computer and Information Science, ICIS 2008 (2008)
26. Islam, R., Wanlei, Z.: Email Categorization Using Multi-stage Classification Technique. In: Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2007 (2007)
27. Kun-Lun, L., et al.: Active learning with simplified SVMs for spam categorization. In: Proceedings of International Conference on Machine Learning and Cybernetics (2002)
28. Zhen, Y., et al.: Application of the Character-Level Statistical Method in Text Categorization. In: 2006 International Conference on Computational Intelligence and Security (2006)
29. Jindal, N., Liu, B.: Analyzing and Detecting Review Spam. In: Seventh IEEE International Conference on Data Mining, ICDM 2007 (2007)
30. Guoyang, S., et al.: Detecting Link Spam Using Temporal Information. In: Sixth International Conference on Data Mining, ICDM 2006 (2006)
31. Sirisanyalak, B., Somit, O.: An artificial immunity-based spam detection system. In: IEEE Congress on Evolutionary Computation, CEC 2007 (2007)
32. Dhinakaran, C., Chae, C.-J., Lee, J.-K.: An Empirical Study of Spam and Spam Vulnerable email Accounts. In: Future Generation Communication and Networking, FGCN 2007 (2007)
33. Qiu, X., Hao, J., Chen, M.: Flow-based anti-spam. In: Proceedings IEEE Workshop on IP Operations and Management (2004)

34. Ahn, S.-I.: Background Paper For The OECD Workshop On Spam (2004), doi: DSTI/ICCP(2003)10/FINAL
35. Hoanca, B.: How good are our weapons in the spam wars? IEEE Technology and Society Magazine 25(1), 22–30 (2006)
36. Yang, L., Bin-Xing, F., Li, G.: TTSF: A Novel Two-Tier Spam Filter. In: Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2006 (2006)
37. Garg, A., Battiti, R., Cascella, R.G.: "May I borrow your filter?" Exchanging filters to combat spam in a community. In: 20th International Conference on Advanced Information Networking and Applications, AINA 2006 (2006)
38. Pelletier, L., Almhana, J., Choulakian, V.: Adaptive filtering of spam. In: Proceedings of Second Annual Conference on Communication Networks and Services Research (2004)
39. Ali, A.B.M.S., Xiang, Y.: Spam Classification Using Adaptive Boosting Algorithm. In: 6th IEEE/ACIS International Conference on Computer and Information Science, ICIS 2007 (2007)
40. Ming, L., Yunchun, L., Wei, L.: Spam Filtering by Stages. In: International Conference on Convergence Information Technology (2007)
41. Brewer, D., et al.: Towards an Ontology Driven Spam Filter. In: Proceedings of 22nd International Conference on Data Engineering Workshops (2006)
42. Chhabra, S., Yerazunis, W.S., Siefkes, C.: Spam filtering using a Markov random field model with variable weighting schemas. In: Fourth IEEE International Conference on Data Mining, ICDM 2004 (2004)
43. Guoqing, M., et al.: Multi-agent Interaction Based Collaborative P2P System for Fighting Spam. In: IEEE/WIC/ACM International Conference on Intelligent Agent Technology, IAT 2006 (2006)
44. Schryen, G.: Approaches Addressing Spam. In: Proceedings of the HHCCII, Hawaii (2004)
45. Pfleeger, S.L., Bloom, G.: Canning Spam: Proposed Solutions to Unwanted Email. Security and Privacy in IEEE, 40–47 (2005)
46. Hunt, R., Carpinter, J.: Current and New Developments in Spam Filtering. In: 14th IEEE International Conference on Networks, ICON 2006 (2006)
47. Banerjee, A.: Architectural Considerations for a World of Devices. The Architectural Journal 14, 2–7 (2007)
48. Xinwen, Z., Onur, A., Jean-Pierre, S.: A trusted mobile phone reference architecturevia secure kernel. In: Proceedings of the 2007 ACM Workshop on Scalable Trusted Computing. ACM, Alexandria (2007)
49. Gavidia, D., et al.: Canning Spam in Wireless Gossip Networks. In: Proc. 4th IEEE Conference on Wireless On Demand Network Systems and Services (WONS). IEEE, Obergurgl (2007)
50. Anand, R., et al.: Securing Mobile Appliances: New Challenges for the System Designer. In: Proceedings of the Conference on Design, Automation and Test in Europe, vol. 12003. IEEE Computer Society
51. Aggarwal, M.: Does SMS text message pose a security risk? News (2010)
52. LightReading, AdaptiveMobile Fights Off SMS spam. LR Mobile News Feed (2011)
53. Weili, H., et al.: Anti-Phishing by Smart Mobile Device. In: IFIP International Conference on Network and Parallel Computing Workshops, NPC Workshops (2007)
54. De Santis, A., et al.: An Extensible Framework for Efficient Secure SMS. In: 2010 International Conference on Complex, Intelligent and Software Intensive Systems, CISIS (2010)