Global Information Assurance Certification Paper

Unsolicited Bulk Email - The problem and some hope

Edward A. Mauro
January 24, 2001

Overview

This paper is intended to explain the problem of Unsolicited Bulk Email (UBE), commonly referred to as "Spam", or sometimes called Unsolicited Commercial Email (UCE). It is directed not only to system administrators, but also to the average person who reads email. In this paper, we will look at the definition of UBE, potential damages, surrounding laws and what can be done to combat this flurry of junk-mail that fills our inboxes with unwanted mail. Keep in mind that not all UBE is sent via the illegitimate methods described in this document. UBE by definition also includes email from legitimate direct marketing campaigns who have legally bought your name. This document will focus on the variety of UBE that is sent by dishonest means.

Definition

Unsolicited Bulk Email (UBE) is by a literal definition, large amounts of electronic mail that were not asked for by the recipient(s). Depending on how far you extend this definition, it can be construed to include everything from a mail with the subject line of "Make money fast while working from home!!" to your uncle sending an advertisement for his new barber shop to the whole family. Many people refer to it as "spam", though the word "spam" is occasionally used for different meanings in different areas of online computing. According to a document[1] by the Internet Mail Consortium entitled *Unsolicited Bulk Email: Definitions and Problems*,

> Unsolicited Bulk Email, or UBE, is Internet mail ("email") that is sent to a group of recipients who have not requested it. A mail recipient may have at one time asked a sender for bulk email, but then later asked that sender not to send any more email or otherwise not have indicated a desire for such additional mail; hence any bulk email sent after that request was received is also UBE.

The problems arising from Unsolicited Bulk Email are two-fold. There is a measurable monetary cost involved with the sending and receiving of such email, as well as the

frustration and mistrust caused to the unwilling recipients. Both are very real costs, and both exist as parts of the overall problem.

To appreciate the full range of damages associated with Unsolicited Bulk Email, follow the path of one batch of such email. This hypothetical batch of email begins with the harvesting of tens of thousands of email addresses. The harvester runs programs (sometimes referred to as "spiders" or "robots") which scan websites, newsgroups and email lists. To supplement this, a website can be created with code capable of tricking unsuspecting web browsers into giving the email address of the user. Using the results of such scans, the harvester creates a CD with all of these email addresses, which is then sold to somebody with an idea for sending out bulk mail. The spammer then downloads a bulk emailing tool from any one of a number of websites. This tool is configured with the IP address of a victim company's mail server which is not properly configured. That mail server allows what is known as "open relay" or "third party relay". It will send mail from anyone, to anyone, without requiring the sender to authenticate as a valid user. The spammer then configures this email program with a false return address, so that anyone who complains about the email will complain to the wrong person. When the spam begins, the victim server is flooded with 50,000 emails destined for people whose addresses were on that CD. The server is unable to handle this large volume properly, since it was not designed for such large capacity, and crashes. (Note that not all servers will crash due to the extra load. This is a somewhat extreme example.) The postmaster of this server spends a full day's work getting to the bottom of the attack, and finally gets the server running again. When it comes back up, the unwanted mails are still in the outbound queue, and the server needs to process these before allowing employees with valid rights to use their own server. By the time the spam leaves this server, the employees have been inconvenienced for two days, the postmaster spent countless hours recovering a crashed server, and there are 50,000 mails leaving this server for people who never asked for them. Each person who gets this mail needs to spend the extra few seconds to download this message to their reader. Some of these people are paying an hourly charge to connect to the Internet. Some are on wireless devices such as cellphones or PDAs, and are using their allotted minutes. Even the people who are taking advantage of a free Internet service are still using time that could be devoted to a more useful activity. After taking the extra time to download this mail, each of the 50,000 recipients now has an email entitled "Info you asked for". Some of them will take the time to read it, others will simply press Delete. Either way, many of them will get angry with the sender and some will reply. Of course the Reply-To address is fake, so this mail goes to the wrong company, bounces back to the victim, and sends a copy to the Postmaster of that domain. By this point, that single batch of email has crashed a server, disrupted mail for valid users, taken up bandwidth on 50,000 people's connections, angered most of them, and taken up the time of people who responded, as well as the Postmaster of a domain that is probably not even related to the originating sender. As you can see, this practice is more than just one more mail in your Inbox, it is a real problem that needs to be addressed.

Courses of Action

The problem of Unsolicited Bulk Email is global, involving many servers, administrators and end-users, therefor the process of combating it needs to be done on many different levels. Opinions differ on the most effective single way, however any combination of the possibilities is better than allowing it to continue unhindered. These techniques are deployed at differing stages of the UBE life cycle, and have various levels of effectiveness. In order to effectively fight UBE, steps must be taken in preparation before the mail is sent as well as a reaction to receiving it. The distinction between the two stages is not always clear, since the reaction of receiving a mail is to defend against it next time something similar arrives. Fighting UBE is an ongoing cycle much like anti-virus efforts. Below are some of the methods for combating Unsolicited Bulk Email:

Method	Effect	Comments
Stop open relay servers	Hinders the spammer's attempts to hide his identity	This helps the global effort, not necessarily the local server/users
Block known open relays	Denies mail from being delivered	Not foolproof, and can block valid email
Block known addresses	Denies mail from being delivered	Spammer can easily change his address
Server-Side Content Filtering	Denies mail from being delivered	Effectiveness depends on the creativity of the Postmaster*
Educate end-users	Limits target addresses, reduces stress, aids Postmasters	
Client-Side filtering	UBE is still delivered, but end-user is better equipped to ignore or forward to appropriate people.	

*Note: Here, the term Postmaster includes any administrator involved in the anti-UBE efforts. In larger companies, the mail server administrator, Postmaster, firewall administrator and security officer can all be different people or even departments.

Stop open relay servers

Many senders of UBE will attempt to use a server other than their own to process the mail. This serves two purposes. It obscures their identity from the recipient, and places the burden of the work on a computer that they don't worry about overloading or crashing. In order for this trick to work, the server needs to allow them. By default, many mail server installations allow what is known as "open relay" or "third-party relay". Simply put, the server will accept mail from anyone, and send it to anyone. A server that is secured against this tactic will only accept mail from authorized users, and only deliver mail that is destined for valid users of that domain. Most major brands of mail servers have features that allow an administrator to prevent their site from being

used as an open relay. Implementing this feature can take anywhere from a few minutes to a few hours, and is a very helpful step in the global effort of preventing UBE. It also protects the server against unauthorized usage which can slow or even crash the machine. According to a recent survey[2] by The Internet Mail Consortium, "over 6% of mail servers that are named in mail addresses allowed relaying in January 2001, a reduction from 17% from a year and a half earlier". Taking into account the large number of mail servers that exist on the Internet, this is still a considerable number of servers which allow the relay. The percentage has gone down, however this study does not present any estimate of the total number of vulnerable servers.

Block known open relays

There are organizations such as Mail Abuse Prevention System LLC (MAPS) which maintain lists of servers that have been proven to be open relays. These types of lists are known as Black Holes. If a message comes into a server, and that server supports, and is configured for black hole listings, the server will check the incoming message for its origin. If it comes from a domain that is listed as a black hole, it will not be delivered. Not every mail server software has the ability to make use of black hole lists. Among administrators of servers which do support it, some decide not to use this method. The chance exists for a server to deny mail from a domain that sends valid email as well as UBE. According to ORBS, an organization that attempts to warn administrators of open relays in hopes of closing the relay, "at least 40% of the mail servers on the Internet" subscribe to the MAPS Realtime Black Hole List (RBL). Subscribing to a service such MAPS RBL takes little effort, and can potentially block a large amount of UBE, at the risk of blocking a small amount of valid email. Alternatively, a Postmaster can choose to maintain their own list of denied servers. This will require a larger effort on their part, not block as many relay sites, and give them more control over the list.

Block known addresses

Most mail servers have Anti-UBE options that can be enabled. When used properly, these can be very effective methods to control the amount of unwanted email that users will receive. These options typically do not take long to enable and configure, and offer a variable success rate depending on the configuration. The reason that success is variable is that the administrator of the site must determine patterns for the server to search for and deny. If the pattern is too general, valid email can be blocked. If the pattern is too specific, many messages will be able to slip through this protection. Note that depending on the server software, several options can be available for a course of action to take if a message fits the pattern defined in the filter. Some packages will automatically drop the message, pretending it never existed. Others can be configured with more detail and reply to the sender with a denial message, or even redirect the message to an administrator who can decide if it should be delivered. (Care should be taken though, if the server is configured to send a denial message. This can be abused by a crafty attacker and create a denial of service on at least one, potentially 2 or more mail servers)

Depending on the environment that the server is being run in, it could be helpful to provide valid users with a listing of what filters are in place. This will help explain what is being done to protect them from unwanted mail. Care should be taken though, that this list does not fall into the hands of the people who send UBE. It would act as a list of the defenses, giving the sender a simple method of defeating the defense.

One way that an administrator can choose to configure their UBE filter is to deny any mail that comes from known spam senders, based on their email address. For instance, if a user claiming to be "sales@sendmejunk.com" repeatedly sends UBE to a given site, the administrator of that site can add a filter to block that address. How much of the address to block is a choice the administrator needs to make. By blocking the entire "sendmejunk.com" domain, other users with possibly valid email will not be able to send mail to this server. On the other hand, if the administrator chooses a more specific filter which blocks "sales@youwantit.com" then the sender merely has to change their email address to defeat this filter. (For example, "sales2@sendmejunk.com" would remain an acceptable address.) Depending on the administrator, this can either be an effective method for blocking spam, or a grand mistake that can block large amounts of valid email. One bit of caution about using email addresses as a parameter for filtering is that a sender can use a fake address and trick the administrator into denying any mail from that domain rather than the domain of the true sender. This can also be applied as a denial of service attack against the domain that the spammer is impersonating.

Server-Side Content Filtering

Another method for filtering incoming email against UBE is to have the server read each incoming email and look for key words or phrases. This is a more effective way to filter email, since most spammers do not change the content of their mail as frequently as the address from which it appears to be sent. In order for this to work, the Anti-UBE option needs to be configured with a list of words or phrases that are deemed unacceptable by the administrator. A few examples of such words or phrases include:

- Any profanity
- "Make money fast!!"
- "Findout About Anyone Fast Now!"
- "Fly an ultralight aircraft for $45"

Using server-side content filtering, any mail which matches the patterns defined by the administrator will be acted upon how (s)he sees fit. This can include dropping the message altogether, placing it in a holding queue to be inspected, returned to the sender with a denial message, or possibly other actions, depending on the server software being run at that site. The same caveat holds true for content filtering as for address filtering. If the patterns are applied improperly, valid mail can be acted on as if it were unwanted. Many administrators set up an email address such as "abuse@youcompany.com" or "spam@yourcompany.com" for their users to forward UBE, in order to provide samples

of email for obtaining filter patterns.

Educate End-Users

The battle against Unsolicited Bulk Email is not waged entirely at the level of servers and firewalls. An educated end-user can also help prevent UBE from continuing. Educating the user about the prevention and handling of UBE will not only serve to reduce their stress when they do get unwanted mail, but will also empower them to help prevent it from recurring.

The end-users of an email system should know several things about UBE, including how their address is obtained, how they can protect their address, how they can help their administrators, and how their administrator is protecting them. Through this education, the end-user should also realize that while the administrator(s) are working to prevent UBE from reaching them, it is highly unlikely that they will ever be 100% successful in blocking it all. Odds are, some piece will slip through the protection.

Within any organization, there are people who will get moderate to heavy amounts of UBE, and there are some who will get none or very little. This is because the senders need to have your email address in order to send you mail. Occasionally, they may attempt to send a flood of mail to every address they can think may exist at a given domain. (e.g.: a list of first names, positions, titles, etc.) More likely, the address was either harvested from a web page, or bought from somebody who the user willingly gave their name and address to, not realizing it would be spread. In the case of harvesting (also known as scavenging), a program was run that searched through large numbers of web pages and newsgroups for anything matching the pattern of xxx@yyyy.zzz. Having your address as a clickable link on a web page makes it much more likely to be harvested, since the programs can identify it easier by the fact that it is enclosed in HTML tags defining it as an email address. When posting to newsgroups, many people attempt to thwart these search programs by inserting text into their address that will confuse the program. For instance, somebody might insert the words "removethis" into their address, making it "myname@removethis.mycompany.com". To a human reading the address, it will probably seem obvious that the extra words don't belong, and should be removed before sending a mail. The programs need to be told to remove such words, and rely on configuration files to do so. Many of these programs are already aware of the phrase "nospam" in an address, and have compensated for it. Be inventive, but remember that it has to be obvious to a human who reads your address. There are other ways that a spammer can harvest your address as well. Some web browsers will easily be tricked into divulging your identity by reading variables in the HTTP headers, such as "REMOTE_USER" and "HTTP From". Others will embed an FTP request into a page, and request that your web browser give your email address for authentication purposes. The spammer then reads his/her FTP log file, and has your address. Many web browsers can be configured not to give the address to such requests. For instance, in recent versions of Netscape the option is found by selecting Edit, Preferences, Advanced, and un-checking "Send email address as anonymous FTP password".

Another way that a spammer can get a user's email address is simply to buy it from another company to whom that user willingly gave it. In this case, the user most likely wasn't aware that it would be shared, sold, or otherwise spread. The user may have signed up for a service or mailing list, and either did not notice, or was not shown a choice to keep their name private. Many sign-up forms are checked by default that the company will be allowed to share or sell your information to other related companies. Users need to be aware of where they give their email address, and be sure that they trust the companies they are giving their information to.

Once an email address is in circulation, it is only a matter of time before UBE begins to arrive. If it is not being filtered at the server level, it will be delivered to that user's inbox. Many major email clients offer a means to filter incoming messages. Some can merely delete them, while others can either move them into predetermined folders, or even forward them to another address such as their local Postmaster. The same caveat applies here as with server-side filtering. The filters need to be carefully balanced between precision and generality to capture the UBE and avoid falsely capturing valid emails.

Users also need to know what is being done at their server to protect them from UBE. By knowing this, they can work with the administrators to provide examples and background information that can prove helpful to the prevention of further abuse. Many administrators ask the users to forward examples to a predetermined address for processing so that it can be included in future server-side filters. Knowing that they are not alone in the fight against UBE also serves to reduce their anger when they do receive an unwanted email.

As part of the education process, the end-user should be reminded that not all UBE is delivered by illegitimate means. Though it seems that most is, there are some direct-marketing campaigns who use legal means to send you advertisements. Most honest direct marketers process their lists through a service called The Direct Marketing Association (DMA). The DMA seeks to encourage honesty in such campaigns, and offers people a place to enter their address in a list where it can be cross-referenced by marketers. By joining this "opt-out" list they tell the direct marketers that they do not wish to have any email sent to them. The incentive for marketers to use this list is to avoid angering people who might otherwise have sought the company out on their own through other means. DMA maintains the list on their own servers, and offers the user privacy. According to their website[3],

> Any marketer that uses this service, sends their list electronically to e-MPS. All e-mail addresses registered with e-MPS are removed from the marketer's list. The "cleaned" list is returned electronically to the marketer

A user adding their name to an exclusion list such as e-MPS only works if the sender is honest and uses the list. Unfortunately, many people who are sending UBE are not legitimate direct marketers and do not honor such requests. Once a spammer has gotten a user's address and sent mail, that user will want to know what (s)he can do about it. At

that point, many people's reaction would be to reply to the sender and request to be removed. (Some UBE have separate directions at the bottom of the mail, in an attempt to make their message appear to be following direct marketing guidelines) If the sender were honest, they probably wouldn't have sent the mail in the first place, so when the user replies to their message it will likely have the opposite effect of what was intended. Rather than grant the request to remove that address, the request merely validates that the address is actively being used, and should be targeted for another round of UBE. Many organizations, including the Federal Trade Commission (FTC) suggest that users never respond to such messages. Instead, users should forward (not copy and paste) the message to an administrator who can use it to create a new filter in order to block it from returning in the future. In the FTC's Consumer Alert entitled "Trouble @ the In-Box", they also request a copy be sent to uce@ftc.gov where it will be saved to help them "assess, first hand, emerging trends and developments in UCE". In a November 1999 document[4], the FTC says that they receive 3,000 to 4,000 new UBE messages each day.

Many end-users and administrators wish to seek legal action against spammers who use their systems and mailboxes. At this point in time, the laws surrounding Unsolicited Bulk Email are not defined well enough to make this easy. The issue exists on a global scale, yet there is no globally accepted law in place to prosecute with. Even on a United States Federal level, the laws are not clear and are still being debated. One law that may someday be a key player in this is US Code: Title 47, Section 227[5] which was originally written to protect against unwanted marketing phone calls and faxes. Bills have been written (and voted down) which would amend Section 227 to include email as well as faxes. Congressman Christopher Smith (R-NJ) wrote "The Smith Bill"[6], formerly known as HR 1748, which was turned down in the 105th session of US Congress in 1998. In HR1748, Congressman Smith wrote a proposed amendment which would make it illegal to

> "... use any computer or other electronic device to send an unsolicited advertisement to an electronic mail address of an individual with whom such person lacks a preexisting and ongoing business or personal relationship,unless such individual provides express invitation or permission..."

Many other legislators have written similar amendments which are pending as of January 2001. The Coalition Against Unsolicited Commercial Email (CAUCE) provides a useful summary[7] of pending and dead bills. Some US states including California and Washington have passed state laws allowing for prosecution of spammers, however these laws are difficult to enforce. The legal system seems to be struggling with the best approach to this issue, and currently has little to offer the average citizen who receives unsolicited email.

Conclusion

For almost as long as email has been in use around the Internet, there have been people taking advantage of its usage to spread their own messages regardless of whether or not

the recipient wanted to read it. Legislation is slowly being created and/or amended to protect users from unwanted email, however those users and administrators need to take action to hinder the progress of such messages. By closing loopholes in mail servers that allow third-party relay, educating users, and placing filters at mail servers, the community can fight this battle at its own level while waiting for legislation to catch up.

References:

- (1) Hoffman, Paul. "Unsolicited Bulk Email: Definitions and Problems." Internet Mail Consortium Report. Oct. 5, 1997

  URL: http://www.imc.org/uce-def.html (January 21, 2001)

- (2) Hoffman, Paul. "Allowing Relaying in SMTP: A Series of Surveys." Internet Mail Consortium Report. Jan., 2001

  URL: http://www.imc.org/ube-relay.html (Jan. 21,2001)

- (3) "The DMA's e-Mail Preference Service" URL: http://www.e-mps.org/en/ (Jan. 21, 2001)
- (4) Bourne Farrell, Claudia. "Unsolicited Commercial E-Mail (Spam) Could Chill Consumer Confidence in Online Commerce: FTC." Nov. 3, 1999

  URL: http://www.ftc.gov/opa/1999/9911/spam.htm (Jan. 21, 2001)

- (5) "Restrictions on use of telephone equipment." US Code: Title 47, Section 227 Common Carrier Regulation. Jan. 5, 1999.

  URL: http://www4.law.cornell.edu/uscode/47/227.html (Jan. 21, 2001)

- (6) Smith, Christopher. "Netizens Protection Act of 1997." URL: http://www.cauce.org/legislation/smithbill.shtml (Jan. 21, 2001)
- (7) "Pending Legislation" URL: http://www.cauce.org/legislation/index.shtml (Jan. 21, 2001)

- The best plan for a user who receives Unsolicited Bulk Email is to:
  - A) Delete it and move on
  - B) Reply to the sender and request to be removed from the list
  - C) Forward it to the Postmaster of the domain it claims to come from

- D) Forward it to their own Postmaster

Answer: D) Forward it to their own Postmaster

- The approximate percentage of mail servers which are open relays as of January 2001 is:
  - A) 1%
  - B) 6%
  - C) 43%
  - D) 76%

Answer: B) 6%

- Between July 1999 and January 2001, the percentage of mail servers which are open relays has:
  - A) Risen by 12%
  - B) Dropped by 12%
  - C) Dropped by 17%
  - D) Risen by 4%

Answer: C) Dropped by 17%

- In the context of Unsolicited Bulk Email, a Black Hole is:
  - A) An email address that accepts what it is given and ignores it rather than delivering it to a user
  - B) A mail server that is open for relay, and hence is ignored by other servers
  - C) An IP port that accepts what it is given and ignores all packets without giving errors
  - D) A mail server that does not accept any SMTP connections

Answer: B) A mail server that is open for relay, and hence is ignored by other servers

- According to the Open Relay Behaviour-modification System (ORBS), how many mail servers use Realtime Black Hole Lists?
  - A) 20 %
  - B) 40%

- C) 60%
- D) 80%

Answer: B) 40%

- True or False? Replying to a Unsolicited Bulk Email with the keyword "Remove" is an effective way of getting off that sender's list.
  - FALSE - Most times, that only lets them know you're a valid address, so they're more likely to use you again

- True or False? Unsolicited Bulk Email is covered by US Code: Title 47, Section 227, the "Junk Fax Law"
  - FALSE - There have been a few attempts to amend this law to include email, but as of January, 2001 they have all been turned down

- True or False? Recipients of Unsolicited Bulk Email can help prevent it from continuing rather than simply delete it.
  - TRUE - Even if their provider is doing nothing, they can still forward a copy to uce@ftc.gov, as well as the postmaster at the sending server.

- True or False? There are legitimate senders of Unsolicited Bulk Email who will honor a "Remove" request.
  - TRUE - While there are far fewer honest senders that dishonest, UBE is sometimes done by respectable direct-mail marketing campaigns

- True or False? In order for senders of Unsolicited Bulk Email to get your address, you have to have given it to somebody, who then passed it along.
  - FALSE - Your address can be harvested from websites or newsgroups, as well as grabbed from your web browser's configuration during a visit to a website designed to ask for it.