Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft ARTICLE 19
Intended status: Informational G. Perez de Acha
Expires: April 19, 2018 Derechos Digitales
C. Cath
Oxford Internet Institute
October 16, 2017

Unrequested Communications
draft-tenoever-hrpc-unrequested-00

Abstract

This document addresses the topic of unrequested traffic in the form of spam or DDoS attacks. Instead of solely discussing these topics from a mere technical angle, it also addresses human rights implications of unrequested traffic.

Table of Contents

1. Introduction

While researching the human rights impact of the Internet infrastructure we came across several cases which called upon the need to balance rights. The balancing of human rights [UDHR] [ICCPR] is a process in which two conflicting rights, or two uses of the same right, need to be reconciled.

We will specifically look at Distributed Denial of Service (DDoS) attacks as well as unwanted messaging such as spam.

2. Glossary

3. Research Questions

Overal question:

- Should the IETF develop or change its position on unrequested messaging

Specific questions

- Are Distributed Denial of Service (DDoS) attacks a legitimate form of online protest protected by the right to freedom of speech and association?

- Is spam a legitimate way of making use of the right to freedom of expression?

4. Analysis

4.1. DDOS Attacks

Are Distributed Denial of Service (DDoS) attacks a legitimate form of online protest protected by the right to freedom of speech and association? Can they be seen as the equivalent to 'million-(wo)men marches', or sit-ins? Or are they a threat to freedom of expression and access to information, by limiting access to websites and in certain cases the freedom of speech of others? These questions are crucial in our day and age, where political debates, civil disobedience and other forms of activism are increasingly moving online.

Many individuals, not excluding IETF engineers, have argued that DDoS attacks are fundamentally against freedom of speech. Technically DDoS attacks are when one or multiple host overload the bandwidth or resources of another host by flooding it with traffic, causing it to temporarily stop being available to users. One can roughly differentiate three types of DDoS attacks: Volume Based Attacked (This attack aims to make the host unreachable by using up all it's bandwith, often used techniques are: UDP floods and ICMP floods), Protocol Attacks (This attacks aims to use up actual server resources, often used techniques are SYN floods, fragmented packet attacks, and Ping of Death [RFC4949]) and Application Layer Attacks (this attack aims to bring down a server, such as the webserver).

In their 2010 report Zuckerman et al argue that DDoS attacks are a bad thing because they are increasingly used by governments to attack and silence critics. Their research demonstrates that in many countries independent media outlets and human rights organizations are the victim of DDoS attacks, which are directly or indirectly linked to their governments. These types of attacks are particularly complicated because attribution is difficult, creating a situation in which governments can effectively censor content, while being able to deny involvement in the attacks [Zuckerman]. DDoS attacks can thus stifle freedom of expression, complicate the ability of independent media and human rights organizations to exercise their right to (online) freedom of association, while facilitating the ability of governments to censor dissent. When it comes to comparing DDoS attacks to protests in offline life, it is important to remember that only a limited number of DDoS attacks involved solely willing participants. In most cases, the clients are hacked computers of unrelated parties that have not consented to being part of a DDoS (for exceptions see Operation Abibil [Abibil] or the Iranian Green Movement DDoS [GreenMovement]).

In addition, DDoS attacks are increasingly used as an extortion tactic, with criminals flooding a website - rendering it inaccessible - until the owner pays them a certain amount of money to stop the attack. The costs of mitigating such attacks, either by improving security to prevent them or paying off the attackers, ends up being paid by the consumer.

All of these issues seem to suggest that the IETF should try to ensure that their protocols cannot be used for DDoS attacks. Decreasing the number of vulnerabilities in the network stacks of routers or computers, reducing flaws in HTTPS implementations, and depreciating non-secure HTTP protocols could address this issue. The IETF can clearly play a role in bringing about some of these changes, and has indicated in [RFC7258] its commitment to mitigating 'pervasive monitoring (...) in the design of IETF protocols, where possible.' This means the use of encryption should become standard. Effectively, for the web this means standardized use of HTTPS. The IETF could redirect its work such that HTPPS becomes part-and-parcel of its standards. However, next to the various technical trade-offs that this might lead to it is important to consider that DDoS attacks are sometimes seen as a method for exercising freedom of speech.

DDoS although disruptive, and silencing at times, can also enable as protest and speech. Or as Sauter [Sauter] argues: 'though DDoS as a tactic is still relatively novel, it fits within a centuries-long tradition of breaking laws and disrupting business as usual to make a political point. These actions aren't simply disruption for disruption's sake. Rather they serve to help the activist or dissenter to direct the attention of the public through the interpolation of difference into routine.' (30-31). An often heard argument against DDoS attacks is that you cannot construe it as a means to exercise your right to freedom of speech, when the means used effectively impede the right of the party on the receiving end of the attack to exercise that same right. The problem with this line of argumentation is that it conveniently ignores the fact that online DDoS attacks are often one of the few effective ways for activists to gain the attention of the media, the government or other parties of interest. Simply putting up a website for a cause won't garner the same amount of attention as directly confronting the issue via the website of the individual or organization at the heart of the issue. The ability of activists to do so should be protected, especially considering the fact that as Sauter (2014:4) explains: 'Collectively, we have allowed the construction of an entire public sphere, the Internet, which by accidents of evolution and design, has none of the inherent free speech guarantees we have come to expect. Dissenting voices are pushed out of the paths of potential audiences, effectively removing them from the public discourse. There is nowhere online for an activist to stand with her friends and her

sign. She might set up a dedicated blog--which may or may not ever be read--but it is much harder for her to stand collectively with others against a corporate giant in the online space.' Although the Internet is often compared to public space, it is not. Rather the opposite. The Internet is almost entirely owned by private entities. And the IETF plays a crucial role in developing this privatized commercialized Internet.

From a legal and political perspective, the IETF does not have the legitimacy to determine when a DDoS is legitimate (in legal or political terms). It does not have the capability to make this judgment as a matter of public policy and subsequently translate it to code. Nor should the IETF try to do so. From a technical perspective, the difference between a 'legitimate' and 'illegitimate' DDoS attack is meaningless because it would be extremely difficult for the IETF to engineer a way to detect that difference. In addition, there is a need for the IETF to be consistent in the face of attacks (an attack is an attack is an attack) to maintain the viability of the network. Arguing that some DDoS attacks should be allowed, based on the motivation of the attackers complicates the work of the IETF. Because it approaches PM regardless of the motivation of the attackers (see [RFC7258]) for reasoning), taking the motivation of the attackers into account for DDoS would indirectly undermine the ability of the IETF to protect the right to privacy because it introduces an element of inconsistency into how the IETF deals with attacks.

David Clark recently published a paper warning that the future of the Internet is in danger. He argues that the private sector control over the Internet is too strong, limiting the myriad of ways in which it can be used [Daedalus], including for freedom of speech. But just because freedom of speech, dissent, and protest are human rights, and DDoS is a potential expression of those rights, doesn't mean that DDoS in and of itself is a right. To widen the analogy, just because the Internet is a medium through which the right to freedom of expression can be exercised does not make access to the Internet or specific ICTs or NCTs a human right. Uses of DDoS might or might not be legitimate for political reasons, but the IETF has no means or methods to assess this, and in general enabling DDoS would mean a deterioration of the network and thus freedom of expression.

In summation, the IETF cannot be expected to take a moral stance on DDoS attacks, or create protocols to enable some attacks and inhibit others. But what it can do is critically reflect on its role in creating a commercialized Internet without a defacto public space or inherent protections for freedom of speech.

4.2. Spam, filter bubbles, and unrequested messaging

In the 1990s as the internet became more and more commercial, spam came to be defined as irrelevant or unsolicited messages that were porsted many times to multiple news groups or mailing lists [Marcus]. Here the question of consent is crucial. In the 2000s a large part of the discussion revolved around the fact that certain corporations -protected by the right to freedom of association- considered spam to be a form of "comercial speech", thus encompassed by free expression rights [Marcus]. Nonetheless, if we consider that the rights to assembly and association also mean that "no one may be compelled to belong to an association" [UDHR], spam infringes both rights if an op-out mechanism is not provided and people are obliged to receive unwanted information, or be reached by people they do not know.

This leaves us with an interesting case: spam is currently handled mostly by mailproviders on behalf of the user, next to that countries are increasingly adopting opt-in regimes for mailinglists and commercial e-mail, with a possibility of serious fines in case of violation.

While this protects the user from being confronted with unwanted messages, it also makes it legally and technically very difficult to communicate a message to someone who did not explicitly ask for this. In public offline spaces we regularly get exposed to flyers, invitations or demonstrations where our opinions get challenged, or we are invited to consider different viewpoints. There is no equivalent on the Internet with the technical and legal regime that currently operates in it. In other words, it is nearly impossible to provide information, in a proportionate manner, that someone is not explicility expecting or asking for. This reinforces a concept that is regularly discussed on the application level, called ’filter bubble’: "The proponents of personalization offer a vision of a custom-tailored world, every facet of which fits us perfectly. It’s a cozy place, populated by our favorite people and things and ideas." [Pariser]. "The filter bubble’s costs are both personal and cultural. There are direct consequences for those of us who use personalized filters. And then there are societal consequences, which emerge when masses of people begin to live a filter bubbled-life (...). Left to their own devices, personalization filters serve up a kind of invisible autopropaganda, indoctrinating us with our own ideas, amplifying our desire for things that are familiar and leaving us oblivious to the dangers lurking in the dark territory of the uknown." [Pariser].

It seems that the ’filter bubble’-effect can also be observed at the infrastructure level, which actually strenghtens the impact and thus hampers the effect of collective expression. This could be

interpretated as an argument for the injection of unrequested messages, spam or other unrequested notifications. But the big difference between the proliferation of such messages offline and online is the investment that is needed. It is not hard for a single person to message a lot of people, whereas if that person needed to go house by house the scale and impact of their actions would be much smaller. Inversely if it were a common practice to expose people to unwanted messages online, users would be drowned in such messages, and no expression would be possible anymore. Allowing illimited sending of unsolicited messages would be a blow against freedom of speech: when everyone talks, nobody listens.

Here the argument is very similar to DDoS attacks: whereas one could argue for legitimate uses in limited specific cases, these would be drowned out by a malicious use which constitutes an attack on the internet infrastructure and thus the assembly or association itself.

5. Conclusion

While there might be narrow individual cases in which DDoS attacks or spam could be used to rightfully excercise freedom of expression, overal DDoS and spam are a self-defeating practice which harms both the Internet infrastructure and freedom of expression.

The growing use of spam and DDoS attacks also leads to an increased dependency of website owners to rely on third party services for DDoS protection which leads to centralization and thus hampers the resilience of the Internet. Furthermore the increase in spam attacks makes it harder for individuals to run a mailserver because of risks for hijacking and blacklisting of the mailserver, as well as the difficulties in filtering spam from messages that are actually wanted.

6. Security Considerations

As this draft concerns a research document, there are no security considerations.

7. IANA Considerations

This document has no actions for IANA.

8. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research Group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hrpc

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hrpc/current/index.html

9. References

9.1. Informative References

[Abibil] Danchev, D., "Dissecting 'Operation Ababil' - an OSINT Analysis", 2012, <http://ddanchev.blogspot.be/2012/09/dissecting-operation-ababil-osint.html>.

[Daedalus] Clark, D., "The Contingent Internet", Daedalus Winter 2016, Vol. 145, No. 1. p. 9-17 , 2016, <http://www.mitpressjournals.org/toc/daed/current>.

[GreenMovement] Villeneuve, N., "Iran DDoS", 2009, <https://www.nartv.org/2009/06/16/iran-ddos/>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and the first amendment", 1998, <http://www.cardozoaelj.com/wp-content/uploads/2013/02/Marcus.pdf>.

[Pariser] Pariser, E., "The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think", Peguin Books, London. , 2012.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[Sauter] Sauter, M., "The Coming Swarm", Bloomsbury, London , 2014.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <http://www.un.org/en/documents/udhr/>.

[Zuckerman]
Zuckerman, E., Roberts, H., McGrady, R., York, J., and J. Palfrey, "Report on Distributed Denial of Service (DDoS) Attacks", The Berkman Center for Internet and Society at Harvard University , 2010, <https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf>.

9.2. URIs

[1] mailto:hrpc@ietf.org

Authors' Addresses

Niels ten Oever
ARTICLE 19

EMail: niels@article19.org

Gisela Perez de Acha
Derechos Digitales

EMail: gisela@derechosdigitales.org

Corinne Cath
Oxford Internet Institute

EMail: corinnecath@gmail.com