Denials of Service

Jussi Parikka

This article addresses denial-of-service attacks as one key entry point to understanding contemporary issues in network politics. By way of underlining the spiraling feature of the Internet economy as based on security and attack services, it leads into discussing the December 2014 DoS attack against Sony and Xbox gaming networks which were resolved by Kimdotcom offering the hackers vouchers for his file-sharing service, Mega. The article considers the implications of this and other examples in the context of how service has also come to denote a relationship to Internet infrastructure: Servers and the speed of Internet connections that can be slowed down or flooded by way of denial-of-service attacks.

Assumed Service

Service can be considered a general term that designates one major axis of network politics. Software is a service on so many levels. It is, after all, under the rubric of service that one enters into platforms and their terms of use; is granted or denied access to content such as newspapers, media or other things behind a paywall; gets connected on social networks such as gaming network and other forms of fun that, too, are a service. As by the end of this short text becomes clear, *denial-of-services* (DoS) are also services—and they can also be tackled with the further provision of service vouchers. The software-based economy is one of competing services whether we are talking of the official platforms such as social media or the more informal, sometimes criminal, services such as DoS.

Service also implies key cognitive and social skills as the site of extracting value and monetisation. It is, after all, in the service economy that services are effectively invented as ways of accessing your needs, relations and other forms in which value might be discovered. The social is not merely about the factory, as we learned in the post-Fordist political theory; the social is also a service as long as one is able to package it as such. In other words, in the contemporary social media and service economy, the social is accessed as a service.

Besides being a nexus of such relations, where the social and the economic conflate, one can approach service through another link. In terms of technological culture and technological (media) systems, one can follow in the footsteps of Paul Virilio and Wolfgang Schivelbusch in starting to track the nature of technological systems through their breaking points. With the invention of the train comes the train wreck, the history of aviation is one of a systematic relation to the air craft accidents and similarly across a range of technological inventions, one can write the history of their specific accidents. One can write the media archaeology of technology through its breaking points and

analyze how, for example, computers, software and networks such as the Internet, look if one starts from their specific forms of accidents. One can claim that computer worms and viruses have been one such central form of an accident that unfolds the wider logic and implicit infrastructural desires of network culture in relation to universal communicability, exchange and sharing (Parikka 2007; Cohen 1986). This suggests that one can also address the issue of services from the perspective of denial-of service attacks, one recurring/repetitive form of software-based practice that has been coined both as a new form of new political activism and as much as harmful hacking.

Through DoS activities, the idea of services as the mask of software becomes one related to security and commerce. In short, denial-of-service attacks have become part of the vocabulary of media reports and security evaluation of Internet culture since the latter half of the 1990s. In simple, rather non-technical terms, denial-of-service attacks work by bombarding a specific address and its server. The Internet economy of "pings" and "hits" is turned against itself by a technically-induced surge in "popularity" over a short period of time, causing the server to crash and become unavailable. The whole attack has a curious relation to the time of the Internet "pings" (see Pias 2011) and the time-critical infrastructure of the Internet (Ernst 2013) in terms of producing a request time out; or in other words, producing a situation of technical inability to handle requests (being flooded, a situation of service desk management under extreme customer inflow, so to speak). Situations of bureaucracy and customer service turn into problems of Internet traffic and its protocological management, just like social situations of services and servantry have turned into both symbolic signs and cultural techniques of the software search economy (Krajewski 2010). Software turns around the axis of service, whether providing or denying service.

Cultural Techniques of Denial

As writers such as Finn Brunton (2013) have explained, DoS or *distributed-denial-of service* (DDoS) attacks using botnets, are a feature of the history of malicious software. As early as the late 1980s and early 1990s, dangers of worms and viruses were identified in the context of commercial transactions, communication and services. Security measures extended to insurance with Lloyds of London in 1989 already offering packages for network-related incidents. The policy was to cover against loss of telecommunications, software and data faults, as well as virus attacks. Around the same period, Control Risks Group Ltd. formed a new company called Control Risks Information Technology Ltd. (CRIT), which was tasked with combatting computer crime, including espionage, fraud, malicious or illegal data modification, and denial- or destruction-of-services (Parikka 2007, 73). In the unending spiral of the service economy, this situation refers to a service to cover against loss of service.

Worms such as Mydoom (2004) and many others have become milestones in this alternative history of the Internet service economy (read through its underbelly). However, the various cultural techniques of actually denying a service, are even more abundant, including smurfing and fraggling as ways to enforce bandwidth consumption, ICMP (*Internet Control Message Protocol*) echo request/reply pinging, and even by sending single malicious packets such as the Invite of Death attacks using the Internet telephony protocol (VoIP). Such techniques relate to the protocological nature of the Internet (Galloway 2004) but also open up as specific ways of emphasizing the issue of service over software. Of course, when it comes to issues of service and their denials, through a DoS perspective one starts to appreciate how even zombie networks of bots are part and parcel in the formation of the service relations of Internet platforms. A thousand captured machines pinging your favorite games service network is the call of the half-dead slowing down your bandwidth.

This primacy of service and its denial is an interesting feature in terms of software-related techniques. Indeed, it is one way of beginning the task of unfolding the peculiar emphasis on Internet sociability as one of relations of service. For there to be denial-of-service, an assumption of service has to be established as one prime feature of the social digital networks and its platforms. The discourse of services is actually a way of starting to consider whether, instead of software, the issues highlighted and at the centre of this sort of Internet "politics" are ones of servers, not software; of data traffic and speeds, not programs? Naturally one should not consider these things as binary opposites, but when referring to software politics, software studies, and other related terms, one has to remember that not all of the software focus refers back to end user programs, but the wider infrastructural questions and their service relations which sustain the specific modes of subjectivity in network economies: servers, servants, services and their customers (see Krajewski 2010 and 2013 for a thorough media history of servantry).

It is in this context, that the relation of service to "network politics" is emphasized with a twist. The service-induced bracketing of software—there is no software, only services—is a feature that can be addressed by way of analyzing the logic of DoS and service as a feature negotiated as part of Internet infrastructure: servers, bandwidth, slowness and speeds of pings, etc. Services offer access to content, but are also underpinned by how such content and the affective/cognitive economy is reliant on infrastructure. Over the past years, issues of *net neutrality* have dictated a major chunk of the debate on network politics: who is allowed to dictate Internet speeds, potential offering a fast lane to the best paying services over less wealthy users?

DoS offers a further commentary as to the speed and slowness as services. One can even buy this slowing down as a service by way of hiring suitable hacker groups (Brunton 2013; Dredge 2014), just like one is offered services of "neighborhood watch" of distributed webmasters, data management and distributed

clouds to ensure the accessibility of your site even for individuals or small groups/companies (e. g. CloudFlare 2015). Security services extend from mere protection against malicious software to encompass visitor management, content distribution across servers, and traffic optimization.

In any case, all of this illuminates the various levels at which service operates from the service one buys and assumes in terms of content, feeling, user satisfaction and such end-user customer contexts, but also the infrastructural level involved in a network relation: for example, the assumed speed.

Voucher Solutions

As an example of the curious twists of the discourse of service and denial-of-service in Internet culture, consider this example from the end of 2014. During the Christmas holidays in 2014, on Boxing Day, the hacker group Lizard Squad claimed responsibility for a denial-of-service attack on the Sony Playstation and Xbox networks. In the middle of the post-Christmas gaming frenzy, the attack brought down the networks, making headlines as the hacking incidents had done earlier in December. The alleged North Korean hacking of Sony reached an odd consumer-centred "political" debate about censorship as it looked like Sony would pull its film *The Interview* from distribution. Of course, the Sony hack by the group Guardians of Peace focused primarily on capturing a wealth of material from Sony and was different to the Lizard Squad attack.

In a manner that also provides a curious commentary on the notion of network politics, the Lizard Squad situation was resolved by a very surprising mediator, Kimdotcom, the controversial founder of Megaupload, the Mega storage/sharing service and a vocal Internet rights and freedoms activist. According to his own testimony, the hackers were offered vouchers for premium Mega Lifetime accounts in exchange for ending the attack and promising never to do it again.

The situation was resolved with both sides releasing Twitter statements.

Lizard Squad (@lizardmafia) commented in a very satisfied tone:

> "Thanks @KimDotcom for the vouchers--you're the reason we stopped the attacks. @MegaPrivacy is an awesome service."

The happy tone was echoed by Kimdotcom on Twitter: "Xbox Live and PSN services coming back. Many regions fully restored. Full recovery imminent. Enjoy your gaming holidays. You're welcome :-)"

Later on the same day, December 26, 2014, "Remember... Lizard Squad only gets the benefit of free Mega premium accounts if they don't attack Xbox Live & PSN again. #Thatsthedeal".

This did not, however, stop Lizard Squad from offering their services as a separate DDoS-tool called the LizardStresser that one could hire for Internet attack needs: "LizardStresser's highest level of attack promises 30,000 seconds—just over eight hours—for $129.99 a month or $500 for for 'lifetime' usage" (Dredge 2014).

Besides DDoS as a service, the case of the Mega storage/sharing platform is also a curious commentary on the Internet economy. As part of the new vanguard of Internet hero sort of politics of individual cult-producing freedom fighters (alongside, for example, Julian Assange) Kimdotcom's politics-accused-of-piracy has turned to quoting the *Universal Declaration of Human Rights* on the home page of the storage/sharing platform Mega, branded as

> The Privacy Company: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. Everyone has the right to the protection of law against such interference. (Mega 2015a)

Storage and privacy become part and parcel of their business, or more specifically, as specified in Mega's Terms of Service:

> Our service includes UCE [user controlled encryption]. You should keep your encryption keys safe and confidential and not release them to anyone unless you wish them to have access to your data. If you lose or misplace your encryption keys, you will lose access to your data. We strongly urge you to use robust anti-virus and firewall protection. (Mega 2015b)

Significantly, as hacking and related techniques have been adopted as part of the discourse of network politics over the past years, it can also refer to a service-oriented "politics" or "diplomacy" that counters denials-of-service with access to service. Kimdotcom's offer (#thatsthedeal), counters the hacker actions by a Christmas gift of free encrypted storage vouchers ensuring access to gaming network services for millions of users. The culture of vouchers, from shopping and even the privatization of service economies in the wake of austerity policies, signify the ability to choose to be cherished by neoliberal discourse.

Anyhow, in our case, it marks a variation of "there is no software, there are just services" to "there is no software, just vouchers"—a quasi-political service-oriented solution to problems of denials-of-service.

Many thanks to Geraldine Juárez for her feedback and ideas.

Bibliography

Brunton, Finn. 2013. *Spam. A Shadow History of the Internet*. Cambridge, MA: MIT Press.

Cohen, Frederick B. 1986. *Computer Viruses*. A Dissertation presented at the University of Southern California, December.

CloudFlare. 2015. "Give us five minutes and we'll supercharge your website." *CloudFlare, Inc.* Accessed May 28, 2015. https://www.cloudflare.com/.

Dredge, Stuart. 2014. "Lizardsquad now helping anyone copy its Playstation and Xbox attacks." *The Guardian*, December 31. Accessed May

28, 2015. http://www.theguardian.com/technology/2014/dec/31/lizard-squad-ddos-service-playstation-xbox-lizardstresser.

Krajewski, Markus. 2010. "Ask Jeeves. Servants as Search Engines." *Grey Room* 38 (Winter): 6–19.

Krajewski, Markus. 2013. "The power of small gestures: On the cultural technique of service." *Theory, Culture & Society* 30 (6): 94–109.

Mega. 2015a. "Info." *MEGA: The Privacy Company*. Accessed May 28, 2015. https://mega.co.nz/#info.

Mega. 2015b. "Terms of Service." *MEGA: The Privacy Company*. Accessen May 28, 2015. https://mega.co.nz/#terms.

Parikka, Jussi 2007. *Digital Contagions. A Media Archaeology of Computer Viruses*. New York: Peter Lang.

Pias, Claus 2011. "The Game Player's Duty. The User as the Gestalt of the Ports." In: *Media Archaeology. Approaches, Applications and Implications*, edited by Erkki Huhtamo and Jussi Parikka, 163–183. Berkeley: University of California Press.