The ISP Column
A monthly column on all things Internet

The Trashing of the Commons

October 2003

Geoff Huston

The Internet has often been compared to the Commons, where a communal resource was owned by noone, yet it was commonly used to the benefit of all. It is not the concept of the commons itself that has become entrenched in our vocabulary, but the aspect of the "tragedy of the commons", where the unmanaged common resource was abused to the point of destruction. Each individual user stood to gain more through increasing their use of the common resource, and, as there was no governance of each individual's use of the resource, there was no penalty imposed for overuse. No single person or entity was responsible for the proper maintenance of the commons and the cumulative problem of degradation of the resource to the point of collapse was not a problem that any individual user was equipped to tackle.

In old English law the "commons" were areas of land that were held in common by the general population, "the commoners," as opposed to specific tracts that were held by the nobility. The grounds may have been pasture lands, woodlands, or open space used by the general population. The word "commons" is derived from Latin "communis" and means the quality of sharing by all or many.

Fourteenth-century Britain was organized as a loosely aligned collection of villages, each with a common pasture for villagers to graze horses, cattle, and sheep. Each household attempted to gain wealth by putting as many animals on the commons as it could afford. As the village grew in size, more and more animals were placed on the commons, and the overgrazing ruined the pasture. No stock could be supported on the commons thereafter. As a consequence, village after village collapsed.

The analysis of this in a social context was explored in depth in the 1960's. These papers can be found at http://dieoff.com/page95.htm

So does this tragedy of the commons sound familiar for the Internet?

Well, in part, yes. The Internet Commons is quickly turning from a valued medium for communal activity into a hostile wasteland.

Too dramatic? Lets look at the state of the Internet commons today.

This year, 2003, has certainly proved to be a watershed year for the Internet. We've seen the massive assault on a number of aspects of the use of the Internet.

Hows your mail lately? What's the ratio of unsolicited junk mail, or spam, to actual useful communication with people you actually want to talk to? While some of the more extreme cases appear to be of the order of 10 spam messages to each 'real' message, its certainly the case that any unprotected active public mail address would be getting somewhere around three to one as a minimum. Other reports indicate that 60% of all email carried on the Internet is spam of one form of another. For many individuals whose mail address has been public for some years spam is now at a point of some 500 messages per day. That's double the rate of some five months ago.

The trend of spam continues sharply upward. What will email look like when the rate of spam is ten times current levels, or higher?

Such a world looks very daunting from where we are. Will anyone be able to publish their email address on the net? How long will an email address be valid for before you have to give it up as hopeless spam- bait and assume a new identity? At what point will the time-wasting overhead of sifting through the trash looking for a genuine message prove too much of a frustration, and users effectively leave email behind as a useless joke? At what level of spam will we have managed to destroy public email as a useful communications medium?

We have already managed to transform one of the more innovative and remarkable communications applications into a pool of digital slime. I'm referring to "usenet", the quite remarkable distributed flooding communications system that carried at first some hundreds, then some thousands of diverse conversation groups. Usenet "news" was perhaps the first effective model of peer-to-peer communications on a truly massive scale. These days the problem is that the original, unmanaged cooperative model of a communal meeting place has been destroyed completely through over-abuse. Efforts to impose some form of administration on usenet have repeatedly collapsed in the bitter acrimony of terminal frustration, and these days its simply not a useful tool any longer. The application has become moribund. IRC, or Internet relay chat, suffered the same dismal fate, and the current set of messaging environments live a shadowed half-life attempting to be well known enough in the community that is attempting to use them, while being not sufficiently well known to become a vulnerable target for fatal abuse.

So with email it may only be a matter of time before the medium gets destroyed by this relentless method of abusive attack.

Of course, annoying as it is, spam is not the complete picture. We need to add to the list an exotic collection of worms, viruses, and related bio- hazards.

Perhaps the major intellectual leap with computing machinery in the mid twentieth century was the so-called Von-Neumann architecture, where instructions to the computer's central processing unit and data that was manipulated by this unit were stored in the same format in the same shared storage system. Turning data into instructions becomes then a case of setting the program counter to the appropriate memory address, and pressing on. Every time a program is run on your computer this step takes place, where data on the disk is transformed into instructions to be executed by your computer. So it should come as no surprise to learn that this became the means of a computer's vulnerability to hostile programs. A virus or worm is injected into a system often by masquerading as data, and the system is then induced to view this data as an instruction set and execute it. And all of a sudden you have a problem.

Not all these spam messages are benign. Some of these messages contain forms of attachments that are destructive. The messages are often constructed in such a manner that induces the unwary to execute the attachment, and others attempt to exploit a vulnerability in a host system that will automatically execute the attachment.

Having your computer system fatally corrupted and losing the entire contents of your file system is not just a remote possibility. Every computer system openly connected to the Internet is being continually probed, sniffed, checked out and tested for vulnerabilities. And it would appear that pretty much every user has fallen prey to this continual assault more than once.

Like any effective biological viral attack, an effective computer virus normally works in a number of phases. Following infection the first task is to embed itself deeply enough in the new host to such an extent that its detection and removal is intended to be thwarted. It then attempts to replicate itself by infecting other hosts. And, either deliberately, or as a result of its deep embedding or aggressive replication, the virus turns on its host system. And you are left wondering why your computer doesn't start up as quickly as it used to when you first bought it, or why things seem 'slower", or why your computer appears to have network activity even when nothing appears to be running, or why your computer simply cannot boot up any more.

How much of the Internet traffic is hostile? How much of the traffic on the network is either the initial attempts to probe the level of vulnerability of remote systems, or the result of infected zombies sending out a further torrent of digital noise? How rapidly can software vendors convey a continuous sequence of patches and updates to applications to counter the efforts of others to exploit vulnerabilities in these systems? How disruptive is the combination of a virus and spam, where the infected host starts to send out virus- infected messages, masquerading as the local system's user, and sending these messages by mail to every party listed in the local user's mail contacts, sometimes even going to the extent of borrowing fragments of stored mail in order to look like genuine mail?

And maybe these are not the central questions. Perhaps the more worrisome question is what does the Internet look like when this traffic increases by factors of 10 or higher over the current levels? How much will this form of abuse collectively cost us, both financially and in terms of an ever-rising sense of impotent frustration?

Again the commons of the Internet falls prey to such hostile abuse.

Not all attacks are directed at the application. Some are directed towards the host system, or even to a part of the network. The intent of such attacks are to swamp the host or network with bogus traffic, and to do so at such an overwhelming level that 'normal' operation simply cannot take place.

The original response was to find a pattern to the attack, and then to place filters either on the host or in the network that discard this traffic prior to reaching its intended destination. The response from the attackers has been to combine this form of attack with viral infection, where the infected hosts would also take on the role of zombie attacker. In this model of a distributed denial of service attack each individual zombie attacker may not be individually sending enough traffic to disrupt the victim, but the cumulative sum of all these attacks, when coordinated, is more than enough to cause damage, And in this case the attack has no discernable pattern or origin.

Right now these attacks come in identifiable waves. There was the 1999 Happy/Ska attack and the Pretty Park and Melissa worms of the same year. The lowlights of 2000 include the Love Letter worm, and in 2001 the Nimda worm. In 2002 the Winevar worm started attacking the antivirus processes on hosts in order to conceal its existence. And this is just a very small sample of the space. The last few weeks of August in 2003 struck a new nadir for the Internet Commons. A combination of the MS Blaster, Welchia and Sobig.F worms struck almost simultaneously.

The increasing concern is how can we rearrange our use of the Internet such that we can avoid increasing exploitation of vulnerabilities in our networked environment, and avoid our communications being overrun by noise.

Internet service providers are increasingly being pushed into a an undesirable position. In order to provide 'normal' service to their clients they have to provision their systems to be able to manage the massive overloads caused by these waves of attack, rather than constructing systems that are dimensioned for 'normal' use. There have been a number of well reported incidents where large public mail server systems have been unable to cope with the torrent of junk mail generated by infected systems that spew out vast quantities of infected mail. The forced response has been to spend additional resources to increase the capacity of the systems to cope with this overhead while still attempting to pass genuine traffic through without hindrance. Whether your role is in provisioning sufficient capacity in DNS servers to handle not only the normal traffic load, but also the additional load imposed by various forms of attack and abuse, or whether you are operating a public mail service where you need to be able to provide sufficient capacity to cope with fluctuations in load where attack peaks can impose overload conditions orders of magnitude greater than genuine message processing rates, you are facing a common problem. We are now dimensioning our servers to handle abuse, not genuine use.

Technical approaches to the problem have so far proved ineffectual. Aggressive attempts by suppliers to fix vulnerabilities often expose these vulnerabilities to subsequent attack, as the user base tends to lag well behind in terms of installing the latest set of updates. Attempts to automate much of this update process have in turn made these update systems the target of attacks, and often expose vulnerabilities that are then used as the basis of subsequent attacks. Attempts by end systems to impose identity- based barriers on incoming transactions, whether its by mail filters or by more sophisticated forms of authentication often fall prey to exploits that assume control of the end system and then become an attack platform using the assumed identity of the host system to break through the identity barriers of other systems within the same web of mutual trust.

And the problem here is that while these remain relatively isolated incidents it is possible to amass a collective response to each wave of attack, but when such attacks increase in frequency and diversity such that's its a continuous effect, such responses tend to be ineffectual.

At a recent IETF open plenary meeting I was interested to read of the plenary topic for discussion. Its worth quoting in full, as it points to a very significant development in our perception of the Internet and the relationship between architecture, use and abuse.

> Open Architecture Discussion Topic:
>
> Are Insecurities at the Edge the Biggest Challenge Yet to the End-to-End Model of the Internet?
>
> When we think of DDOS and Internet-propagated virii, we typically focus on the bad behaviour of the instigator. And, as recent years have seen a massive increase in the amount of malicious and/or unsolicited traffic on the Internet -- denial of service attacks, worms, virii, spam -- we are painfully aware of the costs. Not only end-users are impacted, in the case of spam: anyone setting up mail service has to provision it to handle the amount of traffic it will get, not just the amount of legitimate traffic.
>
> Looking at the rate of increase of these attacks -- e.g., the spike in spam after the SoBig virus was detected -- it seems that the viral nature of propagation has its own set of implications: not only must we deploy countermeasures within the network to avoid the flattening of endpoints under attack, it is increasingly obvious that "endpoints" as we know them cannot be trusted.
>
> If endpoints cannot be trusted, then the proposed longer term solutions for spam that are based on authenticating senders via credentials will not succeed as the only solution. Imagine if you will a situation where if present trends continue we might project seeing things such as the following:
>
> a. Continuous DDOS attacks against the Internet infrastructure.
> b. Releases of multiple CERT advisories **every day**
> c. Virus traffic + spam + patches + file "sharing" traffic comprising the overwhelming fraction of total Internet bandwidth
> d. Organizations restricting or actually **decommissioning** use of email.
>
> The combination of all these trends makes the threat to the end-to-end model from NAT or filtering look fairly minor.
>
> This discussion will include brief presentations outlining some metrics used to determine the trendlines and attempt to determine the current scope of the problem and the slope of the trend line.
>
> The important points for further discussion are:

1. what are some of the additional implications, in terms of work the IETF could and should be doing?
2. since the data shows that a substantial amount of malicious traffic (worms, ddos, virus propagation) is virally generated and operating with the full rights and privileges of some real user, to what extent is conventional authentication & authorization technology useful?

This is not a Tragedy of the Commons in the sense that its not the greed of the individual participants that is driving the Commons into a ruined state. This is more a case of creating a common resource that is showing all the signs of being resistant to policing, and in the absence of such controls that reinforce social behaviours of restraint and care we see instead an environment that is being abused and trashed. This is not a pretty sight.

What are we doing about it?

Like the commons, individual actions in the face of this assault on the commons can only offer some degree of individual mitigation to the problem, again at the expense of the common resource.

An example of this is the increasing use of email filters that attempt to block unwanted messages from reaching your mailbox. Some systems attempt to inspect the mail to detect whether it matches a common profile of a spam message. The problem with this is that spammers use the same systems to attempt to ensure that their message bypasses these generic filters. A slightly more effective approach is to block all messages except those that are sent by a member of a list of people with whom you wish to communicate, a so-called 'white list'. This is also coupled with a more secretive approach to distribution of your own email address, avoiding sending messages into public forums.

So email now becomes a maze of secretive bilateral relationships where each user is forced to maintain individual barriers to withhold the flood of spam. It the telephone directory was the enabler for the social acceptance of the telephone, then what we are doing is trying to make the email directory a collection of semi-private secrets.

And even then it is not that effective. Forging the sender's address is now a common spam technique intended to bypass these individual barriers. And one of the more destructive forms of attack is when your local system is compromised and used to emit a replica of the virus of all addresses in your contact list.

It seems that right now the collection of attackers are better organized and better empowered then the collection of users (or in this case, 'potential victims' is a better word). The attackers are adapting and learning at a rate that easily matches the collective ability of the rest of us to construct effective counter-measures. We need time to better organise ourselves to respond, and time is not a commodity in abundance when looking at the increasing escalation of attack.

Perhaps we need to think about this differently. Perhaps, like the road system, the best we can hope for is to minimize the impact of damage, rather than completely eliminate the possibility of collision.

And here is where the ISPs may well have a role to play. It seems like customers want to have only the 'good' packets and have their service provider filter out the 'evil' packets. Unfortunately the virus and worm writers and bulk mailers haven't implemented all of the provisions of RFC 3514 as yet, so it looks like the task is a significant one. It may well require ISPs building walls and checkpoints within their network, constructing application level gateways, session filters and deploying additional control procedures to permit transit of a limited set of communications to their customers.

The good news for ISPs is that this is what we often call "value-added solutions", and its been something ISPs continually look out for. Its reasonable to expect that ISPs will augment their offerings with various forms of filtering of customer-destined traffic, and will need to assume a role as a delegated agent of the customer in installing customer-specific filters and barriers in their network. It may also include filtering the customer connection to a set of particular applications rather than just "IP" connectivity, and then using application-specific handshakes to provide some assurance that the remote party really is a person with a desire to open a genuine communication channel with the customer. This allows the ISPs to open up a new market in providing a necessary and valuable service to their customers.

Unfortunately this is not completely good news for the Internet Commons as we've come to know it. All this is a step back from the original model of a simple switching network with capable and agile collection of end systems engaging in a peer-to-peer communication environment. As we retreat into our walled gardens of limited trust, install the guards at the gates and control the perimeters with attack dogs, the Internet commons may fall into further neglect. Perhaps intermediary-assisted communications systems are not technically required, but socially they become an simple imperative.

Disclaimer

The above views do not represent the views of the Internet Society, nor do they represent the views of the author’s employer, the Telstra Corporation. They were possibly the opinions of the author at the time of writing this article, but things always change, including the author's opinions!

About the Author

GEOFF HUSTON holds a B.Sc. and a M.Sc. from the Australian National University. He has been closely involved with the development of the Internet for the past decade, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. Huston is currently the Chief Scientist in the Internet area for Telstra. He is also the Executive Director of the Internet Architecture Board, and is a member of the APNIC Executive Committee. He was an inaugural Trustee of the Internet Society, and served as Secretary of the Board of Trustees from 1993 until 2001, with a term of service as chair of the Board of Trustees in 1999 û 2000. He is author of a number of Internet-related books.

E-mail: It might help to reduce his spam load if his E-mail address were only available following a rigorous exchange of credentials!