2010 Global Symposium for Regulators
Dakar, 10 to 12 November 2010

SOURCE: **Information and Communication Technologies Authority of Mauritius**

TITLE: **Challenges to open networks: what strategies?**

Development of a "defense in depth" regulatory framework

Problem statement

Should Internet Service Providers (ISPs) supply their customers with an Internet connection over a network feed that is clean from illegal web content and malware - programs that could cause network lag, compromise system security and threaten user privacy; in the same way that, a water company, in the wide public interest and as a responsible utility provider has to make sure that the water provided in its pipes is uncontaminated and flows securely all the way to their customers' water taps. Should we as regulators, be it through voluntary adoption or regulatory intervention put the onus for such kind of extended 'clean feed' provision as the responsibility of ISPs - and, could that be possible?

Current situation

By shifting some of the burden of security from end users to ISPs, who have more information and are more technically apt, everyone could benefit—ISPs, individual users, and businesses responsible for providing and operating secure networks.

However, barriers preventing ISPs from becoming more involved include a variety of technical costs and legal issues, as well as uncertainty regarding who would meet these costs.

To overcome such barriers, several papers have suggested that government regulations or potential liabilities assigned to ISPs would provide the appropriate motivation to the latter. Others suggest that users might be willing to pay enough to cover these ISP costs.

"Defense in depth" strategy

The need for a clear roadmap where the role and responsibilities of the different groups of stakeholders are defined is now warranted to ensure a holistic approach to handle the multifaceted dimension of cyber threats. In this context, the concept of "defense in depth" strategy which is a well proven one from a cyber security technological standpoint can be put to contribution. The idea behind the "defense in depth" approach is to defend a system against any particular attack using multiple layers of defense. The prime objective of this type of cyber security regulatory framework will be to clarify the role of the regulator with respect to securing access to open networks and also further assert that of the ITU as the international coordination agency on cyber security. Transposition of the same layered approach onto the ICT regulatory framework can add clarity to the responsibilities to be shouldered by each of the stakeholders involved, viz., end users, ISPs and regulators when it comes to tackling cyber threats. However, this "defense in depth" regulatory framework can be clearly defined only if a workable technical and operational set up to combat cyber threats is established. The proposed technical and operational framework can be configured as a shared cyber security infrastructure to ensure cost effectiveness.

Outbound traffic monitoring

The starting premise is that controls implemented by ISPs, focus mainly on protecting their own network— and customer base—from external attacks and therefore predominantly target inbound traffic. However, there is no similar economic incentive to control outbound traffic, as the potential damage is to other networks. This lack of clear lines of accountability derives from both the decentralised nature of routing in the Internet as well as its decentralised organisational structure.

Security controls that focus only on inbound traffic tend to be limited in their effectiveness. Such traffic has already traversed multiple domains and wastefully consumed network resources. Many of the attacks that originate from a single domain rapidly branch out toward many targets, making it much more difficult to control them at destinations rather than sources.

To improve Internet security, it is essential that service providers control outbound as well as inbound traffic. Outbound traffic control stamps out attacks at the source and thus stops them from spreading, without subjecting the network to congestion.

Centralised malware filtering solution

Up to now, agencies such as Computer Emergency Response Teams (CERTs) are geared towards inbound traffic monitoring. The idea in this submission purports to adopt the “defense in depth” regulatory framework by focusing on cyber security measures to be deployed on outbound traffic as another defense layer which will add on to the measures already deployed for inbound traffic. A caveat to be considered in this endeavour is to avoid compromising the quality of service in the deployment of cyber security measures on outbound internet traffic.

For this purpose, we can hinge on a well proven solution deployed for centralised web content filtering which operates as follows:

The system is based on a hybrid Border Gateway Protocol (BGP) and Uniform Resource Locator (URL) filtering system. The first step is where a server containing the list of blocked sites (blacklist) checks the IP addresses of these sites and advertises the routes for these sites to go to a filtering server either within the ISP network or external to it in the case of an externally hosted system rather than the destination web site. The second step is where the filtering server checks the URL against the blacklist using packet inspection and if blocked then the request is not passed on to the destination web site but redirected to a blocking server and displays a block page. If the site is not on the list the filter passes the request as normal and the site is accessed by the ISP customer (“clean traffic”).

This system has the following advantages:

- It has very little effect on the passage of most network traffic so has little effect on performance.
- It has a lower cost than one-step filters that need to filter all of the ISP’s traffic.
- As it does not have a proxy server it does not suffer from the potential problem of requests being changed to the proxy IP address from the customer’s original one.
- As it uses external BGP it can be hosted external to the ISP and is ideal for country gateway implementations

The idea is to extend the use of the above mentioned centralised web content filtering solution to a centralised malware filtering solution for internet outbound traffic which is both technically sound and cost effective. The major challenge to overcome is to ensure minimal network performance degradation in terms of latency with such a solution as malware filtering will use deep packet inspection.

Moreover, this centralised malware filtering solution will need to cater not only for outbound http traffic but for all types of outbound traffic on the Internet through which malware are conveyed. For instance, the use of encrypted channels for access to Internet sites provides an additional shield of the transmitted data, but at the same time, they can be used as channels for malware propagation also. Therefore, https traffic will need to be catered for in this solution. Similarly, other types of traffic such as peer-to-peer, instant messaging, web 2.0 and smtp will also need to be catered for in this proposed centralised malware filtering solution.

Conclusion

In the light of the abovementioned potentials and challenges Mauritius submits for the consideration of the symposium that we use the ITU forum to come up with a standardised protocol to be used for a centralised malware filtering solution. Such a standardised protocol will go a long way to enable the common Internet users to reap the benefits without the need to worry about the complexities of the technology sitting behind such a solution. Once this is done, there will then be the need to map onto it the roles and responsibilities of the stakeholders involved in the “defense in depth” regulatory framework. Here again, the ITU as the international coordination agency for the communications sector is ideally positioned to fulfill this mandate.