Barriers to Deployment: Probing the Potential Differences in Developed and Developing Infrastructure

Karen O'Donoghue and Phil Roberts
The Internet Society

Introduction

There are sometimes differences between network management practices in the developed and the developing worlds. These differences can come from differences in the kinds of devices that are deployed, differences in the nature of connectivity, and differences in the ability of local infrastructure to support localization of content. As the traffic on the Internet becomes more encrypted, these differences can become more obvious as some local optimization techniques are no longer possible.

Our primary interest in this workshop is making sure that the perspective of networks in the developing world are considered, and that any obstacles identified through those perspectives are highlighted in an effort to bring techniques to bear, through the deployment of new technology and the consideration of implementation in public policy, that will remove those obstacles.

We believe it is important to bring two kinds of participants into the discussion: content providers who have knowledge of the performance aspects of delivering content in the developing world and the impacts of encryption on that; and operators of networks in the developing world who deal with the delivery of services and observe the benefits and limitations brought about through increased encryption. We believe that having both of these perspectives will help the Internet rapidly to come to resolution of any remaining obstacles so that everyone can enjoy the benefits of fully encrypted communication.

Although the workshop is specifically identified as a mobile network workshop, many of the issues that we are concerned about apply in both fixed and mobile networks. While some of the technologies to be discussed are unique to mobile network deployments, many of the broader issues in the developing world are not. It would be good to take this workshop as an opportunity to discover those impacts.

We have identified at least three areas where we believe there may be sufficient differences between the developing and developed world that may impact the deployment of encryption: 1) technology availability; 2) localization of content; and 3) the long tail of deployment.

Technology Availability

The technology deployed globally to provide both the Internet infrastructure and the end point access to the Internet varies widely. In particular, the developing world often lags significantly behind the developed world in the capabilities of both its infrastructure and the access devices.

The question that interests us is the impact of this technology gap when encryption is deployed more universally. Will there be a performance or capability impact that will deny some individuals reasonable access to the Internet? How can we gather the right information to make this assessment? What can be done to mitigate this potential impact? While some of these are beyond the scope of managing the network, these are all questions that we feel need to be considered. When is the technology that is deployed in the developing world a limit to what can be made available over encrypted connections in that environment?

Localization of Content

One strategy to improve access to global content, from both an availability and a performance perspective, is to provide that content locally. The use of regional and local infrastructure to cache global content is growing. If this service is provided by the original content provider then it is reasonable to expect the infrastructure is adequate to provide the service. However, if this infrastructure is provided as a service by a local or regional service provider, will they be able to continue to provide this service in an encrypted world? What are the impacts to local content provisioning in an encrypted environment. Will the end result be reduced availability of content to those who have the fewest options for access? How do we ascertain the magnitude of this potential impact, and what remedies are available to address it?

The Long Tail of Deployment

We believe that ubiquitous encryption of communications is the norm that everyone participating in the Internet should aim for. The traffic that is exchanged on the Internet today can often be greatly impacted through implementation of new technologies in a small number of places. Mobile operators have articulated that up to half of the traffic exchanged on their networks is sourced from 3 or 4 major web properties (Google, Facebook, YouTube, Netflix). They have observed that when these properties turned up IPv6, up to half of the traffic on their network moved from IPv4 to IPv6. It may be a similar case with encrypted content on the web today. Some enterprise network operators have observed that up to 70% of the traffic they exchange is occurring over encrypted connections. This is great!

But one must ask: how much encrypted content is enough? Is getting 70% of the traffic exchanged on the Internet to use encryption enough, or do we need to make the long tail encrypted also? Part of the rationale of pervasive encryption is to make pervasive monitoring too expensive for government-sized actors to continue to undertake, and thus resulting in end-users having privacy in their online communications.

It is our belief that enabling some high percentage of encrypted content may discourage government actors attempting to perform pervasive monitoring, but we still envision an Internet where encryption is used to protect all communication for every user of the Internet. We desire full encryption everywhere.

Given then that we would like to make sure that the long tail of content on the Internet enjoys the benefits of encrypted communication, how do we go about removing the barriers to enabling that long tail? We would like to have a discussion that examines what some of these issues are and leads to some concrete proposals for overcoming any obstacles that are identified.

Some of the easily identifiable obstacles are the vast number of endpoints involved in communication on the Internet and what they need to do to enable encrypted communication. When we did World IPv6 Launch the participants quickly identified that the only way to get large swaths of end users using IPv6 was to enable IPv6 by default on the devices they used, whether it was operating systems, home routers or other CPE, of the access network itself. What are the entities that need to have enabled encryption by default and how do we as an industry go about making that happen?

Conclusion

Our interest is in getting the Internet to a better place. We envision a healthy and robust Internet that includes private communications for everyone using it. In this workshop we would like to make sure that the issues we see in the developing world are considered, and that we emerge from the workshop with some hope of developing plans that will move the Internet on a trajectory that allows robust private communications for all its users.