Gmail **Broadband TRAI <broadbandtrai@gmail.com>**

Response to TRAI on Public WiFi networks Consultation of 15th Nov 2016

1 message

Arjun Venkatraman MOJOLAB <mojoarjun@gmail.com> Thu, Dec 8, 2016 at 9:01 AM
To: broadbandtrai@gmail.com

This response is on behalf of the COWMesh community, a group of individuals engaged in enabling communities and individuals in remote locations in connecting to each other and the global Internet using open and low cost technologies and methods. One of the primary solution models we work on are shared WiFi networks where community members can own and operate their own WiFi infrastructure such as home routers and use them to share connectivity with their neighbours, either for free or for a contribution towards maintenance of the common network. These networks can also be used to connect regular TV sets (including old CRT units) to WiFi networks, thereby bringing connectivity within the household where it is more accessible to women and young people.
The authority's intention to enable proliferation of public WiFi networks to boost connectivity in the country is welcomed strongly by the COWMesh community, particularly since the model includes the option of individuals and communities sharing their connectivity. Regarding the implementation of interoperable authentication and payment mechanisms, while we strongly support the setting up of such infrastructure as an option we also see the need to continue to support legacy mechanisms of authentication such as physical verification of identification documents by providers, to enable rapid uptake of the model.

Q1. Is the architecture suggested in the consultation note for creating unified authentication and payment infrastructure will enable nationwide standard for authentication and payment interoperability?

The suggested architecture is overly complex and does not address some of the core issues preventing WiFi proliferation. It limits participation as hot spot providers to only those entities who can afford software and hardware infrastructure required to connect and authenticate with UPI and other similar systems.
The means to share a broadband or other Internet connection using a regular home router are already available and well documented. Anyone with a WiFi router can share their connection with others by simply sharing a password. The issue with proliferation has been primarily that there is no clarity on

1. the fundamental legality of re-sharing/reselling of connectivity
2. limitation and management of liability of the provider (the person sharing their connection) for online activity by a user
3. what format and for what period the providers are required to maintain records of access on a shared connection to assist cybercrime investigations.

The present architecture does not clarify these areas any further.
Therefore while the use of open API interfaces as a means to enable interoperability should be encouraged, we cannot recommend making it mandatory or even the default requirement at this stage.
Hotspot providers should have the option of isssuing users local credentials based on verification of appropriate government backed authentication. Other existing mechanisms such as OTP should also be allowed as alternatives to the API based mechanism, provided the standards for maintenance of access records to support cybercrime investigations are met.
For example, one of the community owned networks we are associated with (COWMesh Hawalbagh & Jyoli, Block Hawalbagh, Distt Almora, Uttarakhand) is a community effort wherein low cost broadband connections available in one village are being shared using household WiFi routers connected in a mesh configuration, across 3 villages. The costs of operating the network are shared by all the users by paying a monthly contribution. The owners of the connection currently keep a copy of each user's government ID proof as a means to identify users of the network in the event of a security breach. Further, the bulk of the userbase in this case is static, meaning that people recognise each other and are in a position to verify their recognition by physically checking the users government issued identification. This type of scenario is replicable in many villages across India, provided

1. the legal aspects relating to liability of access be simple and clear
2. the administrative overhead of registering shared networks be minimized
3. local authentication alternatives such as verification of government ID are allowed in parallel with the proposed architecture.

It is also important to note that in India many individuals often do not have sufficient digital skills to operate a payment interface, but may have sufficient skills to begin learning to navigate the Internet. Necessitating that individuals with

limited digital skills share sensitive identification and financial information on a public network simply to connect to the Internet will severely limit user participation and could also lead to an increase in identity theft and digital financial crime. While the option to link payment, authentication and access may be a useful luxury to many who have the skills and can afford the infrastructure, it should be an option rather than the norm.

Q2. Would you like to suggest any alternate model?
Rather than mandate a particular architecture, it would be ideal if the authority could frame a minimal set of standards for compliance by those wishing to share connectivity with others using WiFi or other means. For example, a central registry of shared internet providers is useful as defined in the paper. Providers should be allowed to use one or multiple modes of authentication, which may be local, i.e. the hostpot provider issues the user a set of local credentials, after physical verification of government ID and possible retention of copies for a period, OTP based as is followed by many existing providers or API based (as described in the paper). In the event that physical verification of government ID is being used as a mechanism, the authority should specify the period for which records of users must be retained after they leave the network.

Q3. Can Public Wi-Fi access providers resell capacity and bandwidth to retail users? Is "light touch regulation" using methods such as "registration" instead of "licensing" preferred for them?
Yes! Licensing is a major bottleneck in the spread of connectivity as it unfairly favours large corporations and muscles out the potential small players. Further many retail broadband consumers have excess bandwidth as their disposal, which they should be allowed to resell for value or share with others to enable more people to get online.

Q4. What should be the regulatory guidelines on "unbundling" Wi-Fi at access and backhaul level?
The unbundling model described in F (16) in the consultation paper can be utilized provided locally verified authentication and independent modes of payment are also supported.

Q5. Whether reselling of bandwidth should be allowed to venue owners such as shop keepers through Wi-Fi at premise? In such a scenario please suggest the mechanism for security compliance
The same model that is currently used for cyber cafes should be extended to shop owners and venue owners sharing or reselling connectivity. As the cyber cafe operators are required to keep records of user access, the same mechanism can be used by venue owners. Ideally, there should be an option to maintain records digitally and the period of retention of records should be within reason and capacity of smaller individual players.

Q6. What should be the guidelines regarding sharing of costs and revenue across all entities in the public Wi-Fi value chain? Is regulatory intervention required or it should be left to forbearance and individual contracting?
The distribution of costs and revenue should ideally be left as open to market interpretation as possible. Telcos and ISPs, however, should ideally be prevented from charging additional fees simply because a connection is shared among many users.

--
Arjun Venkatraman
हैकर (hacker)/浪人(ronin)/Open Solutions Architect, prefer animals to people, jungles to cities and linux to windows
E-mail: arjun@mojolab.org
Mobile: +91 89891 61881 (BHO + Roaming)
Web: http://mojolab.org, http://hackergram.org
Twitter: @themojolab, @arjunven, @hackergram