FCC TAC SECURITY & PRIVACY WORK GROUP

WI-FI HOTSPOT SECURITY RECOMMENDATIONS

INTRODUCTION

This brief paper describes the Security and Privacy Work Group's recommendations regarding Wi-Fi hotspot security. These near term recommendations are focused on encouraging wider deployment of appropriate security protections by hotspot service providers, and the Work Group believes the FCC can play a constructive role in such encouragement. The timing is ripe for this effort, as a new generation of hotspot access technology with enhanced security protections is now being implemented by both network and consumer equipment vendors, and it is anticipated that hotspot service providers will begin to deploy these capabilities starting in 2013. Widespread and rapid adoption of these new capabilities will significantly enhance the security protections available to consumers when they are accessing public hotspot services. The Work Group recommends that the FCC help encourage rapid adoption of these enhanced hotspot security capabilities via one or more FCC-sponsored workshops on Hotspot Security.

BACKGROUND: CURRENT HOTSPOT SECURITY PICTURE

The growth of Wi-Fi in public spaces has been exploding in recent years, and this is expected to continue at a very strong pace. This explosive growth is driven by several factors, including the ubiquity of Wi-Fi in mobile devices like laptops, tablets and smartphones, the investment in Wi-Fi networks by fixed broadband providers as a means to extend their services to subscribers outside the home, and the widening support by mobile operators of Wi-Fi hotspots as a means to offload traffic from congested networks and to improve the end-user experience. In this context, the level of security protection available to users of public hotspots is of growing importance.

Public Wi-Fi hotspots have not historically offered users the same level of security protections available in enterprise and residential Wi-Fi networks. In the case of private Wi-Fi networks for enterprise or government facilities, advanced WPA2™[1] encryption and authentication mechanisms (which have been mandatorily required for all Wi-Fi CERTIFIED™ products since 2006) are typically implemented. In contrast, it is still common for public hotspot service to be offered to users as an "open" network without WPA2 protections and to require browser-based user authentication. Although users of such open hotspots can take steps to protect their data (via, for example, virtual private network features), it would benefit the public in general if greater security protection were widely available for hotspot access.

RECENT AVAILABILITY OF NEW WI-FI HOTSPOT SECURITY CAPABILITIES

Fortunately, there have been recent initiatives within the Wi-Fi industry which, if widely deployed, can significantly expand the availability of enhanced hotspot security. Based on recent standards development within IEEE and other SDOs, and in coordination with major stakeholders in the hotspot vendor and service provider communities, the Wi-Fi Alliance launched its Passpoint™ certification program in June 2012. Along with a variety of other features targeted at improving the overall user hotspot access experience, Passpoint integrates WPA2 encryption

[1] WPA2 (Wi-Fi Protected Access2) refers to the Wi-Fi Alliance's security certification program incorporating 128 bit AES encryption together with a set of designated authentication methods.

and authentication into both network and consumer equipment. Service providers offering Passpoint hotspots will be attractive to consumers due to simplification of the user's hotspot access process, for example with automation of both the service discovery and authentication steps. Such automation of security capabilities, similar to cellular access, is key to driving broad adoption by consumers. Consumer preference for these automated capabilities will help to spur broader adoption by hotspot providers, and thereby the availability of enhanced security for all public hotspot users.

The deployment schedule for Passpoint hotspot services is expected to follow the typical pattern for introduction of new communications capabilities, requiring first that the network equipment vendors implement the necessary features, followed by actual service provider deployments. There are already over 60 products certified by the major equipment vendors, and operators are working on trial deployments.

There are "chicken and egg" challenges that must be overcome before broad adoption of this new hotspot technology can be accomplished. To achieve widespread consumer availability of enhanced Passpoint security, it won't be sufficient to simply have new hotspot capabilities deployed – it will also be necessary for consumer device manufacturers to incorporate Passpoint functions into the typical Wi-Fi devices such as smartphones, tablets, and laptop computers. Ideally this would happen simultaneously with the deployment of the new hotspot capabilities. But although such devices are already beginning to be Passpoint-certified, significant consumer demand for such a capability won't really materialize until Passpoint-enabled hotspots are widely available. Successful initial deployments by lead operators can spearhead the subsequent proliferation of advanced security for all public hotspot users by creating market demand for Passpoint-capable user devices, which will then subsequently encourage deployment by smaller service providers.

RECOMMENDATION: FCC WORKSHOP ON HOTSPOT SECURITY

Because of these recent industry initiatives, the time is right for the FCC, in conjunction with partner industry organizations, to convene one or more workshops covering best practices for deploying Wi-Fi hotspot security. Partner organizations that could help the FCC organize these workshops could include, for example, the Wi-Fi Alliance, the Wireless Broadband Alliance, and GSMA.

The target audience for such a workshop should include not only the large carriers with hotspot business units, but other hotspot service providers as well – such as airport and hotel network providers, and government organizations such as municipalities. The workshops should be webcast, and FCC sponsorship will help to ensure the broadest possible participation beyond the member companies of the industry trade associations, and will emphasize that there is a significant public interest aspect to hotspot security. The speakers should be drawn from the partnering industry organizations, as well as hotspot equipment vendors and service providers.

The primary goals would be to raise awareness of the urgency to address Wi-Fi hotspot security, to help communicate the opportunities now available to the hotspot service providers for improving their user security protections, and to share the experience obtained in early operator deployments with both the general service provider and consumer device communities. Another goal would be to provide a forum for the identification of potential barriers to broad deployment and adoption. The workshop would be an opportunity for open exchange among ecosystem stakeholders, including service providers, network and consumer equipment manufacturers, as well as the industry organizations involved in the specification and certification of these new capabilities. The FCC's sponsorship of such a workshop will promote a broad participation among the key stakeholders and will emphasize that the public interest is well served by improving hotspot security for all consumers.

Immediate next steps towards implementing our recommendation would include workshop planning sessions held between the FCC and industry organization partners, so as to develop the workshop agenda/content and identify potential speakers. An outreach program will need to be developed to reach target participants, particularly those who aren't ordinarily engaged with the FCC. Longer term, additional workshops can be planned as needed, based perhaps on the results obtained via a tracking program that monitors the ongoing deployment statistics. Periodic workshops would serve to gauge and encourage adoption and progress advancing standards. It may also be necessary longer term to update best practices as additional Wi-Fi security capabilities become available and as new threats emerge. Finally, as these enhanced hotspot capabilities start to become more widely available, there will be opportunities for the FCC to include these new security protections in ongoing consumer awareness campaigns to encourage consumers to take advantage of them.