Adoption of Traffic Sniffing Standard Fans WCIT Flames

by Alissa Cooper [1], Emma Llansó [2]
November 28, 2012

Updated December 5

The telecommunications standards arm of the U.N. has quietly endorsed the standardization of technologies that could give governments and companies the ability to sift through all of an Internet user's traffic – including emails, banking transactions, and voice calls – without adequate privacy safeguards. The move suggests that some governments hope for a world where even encrypted communications may not be safe from prying eyes.

At the core of this development is the adoption of a proposed international standard that outlines requirements for a technology known as "Deep Packet Inspection" (DPI). As we've noted several [3] times [4] before, depending on how it is used, DPI has the potential to be extremely privacy-invasive, to defy user expectations, and to facilitate wiretapping.

The adoption of this standard, officially known as "Requirements for Deep Packet Inspection in Next Generation Networks," or "Y.2770" [5] came to light last week during the World Telecommunication Standardization Assembly (WTSA), an international meeting held every four years in which the standards-setting body of the U.N.'s International Telecommunication Union, known as the ITU-T, charts the course of its work. Like most ITU working documents, drafts of the standard are locked behind a password wall and not available to the public. While the final standard will eventually be published, the fact that no draft versions are made publicly available at any point in the process illustrates the lack of transparency of the ITU-T in contrast to other leading global standards organizations [6].

Although the upcoming WCIT has been garnering all the attention lately, the global telecom confab in Dubai actually began last week at WTSA. The approval of the DPI standard provides new evidence of the dangers of WCIT proposals related to mandatory standards and cybersecurity.

Standard Procedure?

The ITU-T DPI standard represents a fairly typical early step in the process of standardizing a technology: the standards participants first agree on what the technology should do before they decide how the technology should work. As such, the ITU-T DPI standard doesn't specify exactly how DPI systems should function. But even so, several of the requirements create a real cause for concern, especially in light of WCIT proposals that would make some ITU-T Recommendations mandatory [7], or transfer authority over cybersecurity matters [8] to the ITU.

The ITU-T DPI standard holds very little in reserve when it comes to privacy invasion. For example, the document optionally requires DPI systems to support inspection of encrypted traffic "in case of a local availability of the used encryption key(s)." It's not entirely clear under what circumstances ISPs might have access to such keys, but in any event the very notion of decrypting the users' traffic (quite possibly against their will) is antithetical to most norms, policies, and laws concerning privacy of communications. In discussing IPSec, an end-to-end encryption technology that obscures all traffic content, the document notes that "aspects related to application identification are for further study" – as if some future work may be dedicated to somehow breaking or circumventing IPSec.

Several global standards bodies, including the IETF [9]and W3C [10], have launched initiatives to incorporate privacy considerations into their work. In fact, the IETF has long had a policy [11] of not considering technical requirements for wiretapping in its work, taking the seemingly opposite approach to the ITU-T DPI document, as Germany pointed out [12] in voicing its opposition to the ITU-T standard earlier this year. The ITU-T standard barely acknowledges that DPI has privacy implications, let alone does it provide a thorough analysis of how the potential privacy threats

associated with the technology might be mitigated.

These aspects of the ITU-T Recommendation are troubling in light of calls from Russia and a number of Middle Eastern countries to make ITU-T Recommendations mandatory for Internet technology companies and network operators to build into their products. Mandatory standards are a bad idea [13] even when they are well designed. Forcing the world's technology companies to adopt standards developed in a body that fails to conduct rigorous privacy analysis could have dire global consequences for online trust and users' rights.

Ironically, although the document contemplates that network operators would decrypt user traffic in order to inspect it, the document's security considerations specify that information extracted via DPI "is required to be protected," and that modification, theft, or loss of such information "may make it unusable for the DPI operations." The idea that adding DPI to a network creates a potential security risk for users – not just for network operators – is utterly absent. In general, the security requirements appear to be very generic, specifying what information needs to be protected without specifying the standards to be used for authentication, confidentiality, or integrity protection. Adding DPI to a network creates a significant new attack vector; thorough threat modelling and mitigation at the standardization phase are more than appropriate – they're absolutely necessary.

WCIT proposals from the Arab States and Africa would seek to create new authority over cybersecurity matters within the ITU, and we've previously explained the drawbacks of this approach [14]. If the technical work produced by the ITU-T fails to acknowledge basic user interests in network security – and to specify comprehensive, robust mitigations against security threats – it further highlights the grave problems with trying to address cybersecurity through a closed, centralized body where ultimate authority rests with regulators and where technical experts and advocates cannot even access draft specifications.

It's not clear whether companies will build new DPI equipment to meet the ITU-T requirements or what further DPI standards the ITU-T will approve. Regardless, the standard approved at WTSA provides further evidence of why proposals for mandatory standards and new cybersecurity authority should be struck down next week in Dubai.

Update: While the official draft of the final Recommendation has yet to be posted (check here [15] for the latest updates), what appears to be an earlier draft [16] is available on the Korean Telecommunications Technology Association site. (Note that this draft contains dozens of pages of appendices, which we understand may have been cut.)

- WCIT
- ITU
- DPI
- cybersecurity

Links:
[1] https://cdt.org/personnel/alissa-cooper
[2] https://cdt.org/personnel/emma-llans%C3%B3
[3] http://www.cdt.org/blogs/alissa-cooper/privacy-risks-isps-using-deep-packet-inspection
[4] http://www.alissacooper.com/wp-content/uploads/2011/10/DPIchapter.pdf
[5] http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=7082

[6] http://open-stand.org/
[7] https://www.cdt.org/blogs/alissa-cooper/2908openstand-underscores-commitment-voluntary-internet-standards-process
[8] https://www.cdt.org/blogs/emma-llanso/0609itu-ill-suited-regulate-cybersecurity
[9] http://tools.ietf.org/html/draft-iab-privacy-considerations-03
[10] http://www.w3.org/standards/webdesign/privacy
[11] http://tools.ietf.org/html/rfc2804
[12] http://www.cept.org/Documents/com-itu/7551/(12)115_Comments-on-recommendation-Y2270-Germany
[13] https://www.cdt.org/files/pdfs/Importance%20of%20Voluntary%20Technical%20Standards.pdf
[14] https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf
[15] http://www.itu.int/en/ITU-T/publications/Pages/latest.aspx
[16] http://committee.tta.or.kr/include/Download.jsp?filename=choan%2F%5B2012-1357%5DY.2770.pdf