Proceedings of the 28th IEEE
EMBS Annual International Conference
New York City, USA, Aug 30-Sept 3, 2006

SaB11.3

Maintaining Security and Privacy of Patient Information

Frank E. Ferrante, MSEE, MSEPP

Abstract

As the global Internet evolves into today's more highly mobile and broadband service offerings, it is anticipated that the applications of new services to support telemedicine and eHealth operations using these offerings will result in increasing healthcare benefits for all and generally a lower cost. The one concern that must be addressed when making these changes is to ensure that security technology keeps up with the changes and provides the means by which satisfaction of HIPAA's privacy regulations can be assured. Consider the application of Wireless Communications in connecting medical professionals and patients through the ubiquitous web access arrangements. New products offered to patients and physicians alike are capable of transmitting vital signs, key blood test results for diabetics, blood pressure data, as well as the higher data requirements of X-Rays, MRIs, ultrasounds, CAT scans, and more. But now things are changing. Cell phones, hotspots (802.11 access arrangements) offer opportunities for others to intercept private information if not protected adequately. Today's security offering for wireless hotspots such as the Wired Equivalent Privacy (WEP) offers some security and privacy but it is known to be broken and useful only temporarily and not for protection of vital medical information protection. Currently, chips are being developed that will offer a much stronger protection for personal wireless networks. This recommended standard, referred to as 802.11i's WPA, is already supported within the Microsoft XP Operating System, and it will be enhanced and approved shortly by the latest recommended version of the standard offering WPA2 - for enterprise applications. The final version of 802.11i (WPA2) addresses practically all the vulnerabilities of WEP and more. However, now things are changing once more. A wideband wireless capability that in all likelihood will supercede WIFI within the next five years will allow up to 75 Mbps data transfer rates and support connections to systems in the range of 30 miles or more under the right conditions. In addition, speeding ambulances and cars traveling at speeds in excess of 70 MPH will be more readily capable of interfacing at the higher data rates WIMAX, the much-awaited technology that is expected to provide wireless broadband services on a Metropolitan Area Network (MAN) scale is going to be the next wave of evolution (802.16). Once more, as was the case for WIFI, where is the security? Will the WIFi security offerings support that needed at these higher rates? All of this is yet to be assured. Thus privacy is once again of concern if the standards are not adequate. As planned however, it is my understanding that the new WPA2 will support both WiFi and WIMax security needs. As technology evolves, security must evolve. And if the manufacturers of products can settle on non-proprietary representative devices to support the needs of the medical field, then all will be fine. If they can't, or won't, then delays will occur. My presentation and discussion today will address some of the detail of this security and the issues yet to be faced in protecting medical and patient information.

Correspondence with the author is through Luis Kun with the IRM College
of the National Defense University, Ft. Lesley McNair, Washington DC,
20319 USA (phone: 202-685-2786; fax: 202-6853827; e-mail: l.kun@ieee.org)

1-4244-0033-3/06/$20.00 ©2006 IEEE.