Report of the High Speed Multimedia (HSMM) Working Group

ARRL Board of Directors
2006 Annual Meeting
January 22, 2004

Members: Dr. John Champa, K8OCL - Chairman
Walt DuBose, K5YFW - Assistant Chairman
Gerry Creager, N5JXS - Hinternet Network Architect
John Stephenson, KD8ODZ - OFDM Modem Project Team Manager
Bob McGwier, N4HY – SDR WG & AMSAT Liaison

ARRL Staff Liaison Ed Hare, W1RFI

1. OFDM Modem Project

OFDM Modem Project Update: John Stephensen, KD6OZH, reports that he is almost done assembling the analog RF boards for the 6M (200 kHz bandwidth for 240 kbps under Experimental Licenses) and the 70cm (2 MHz bandwidth for 2.4 Mbps using streaming digital video in an ATV channel) testing. He should have more to report by the 20th. Most of December was lost due to Christmas and having the flu for a week. John did get a new Luxo microscope on an adjustable arm so assembly is now easier and faster.

RECOMMENDATION: Bandwidth allowed should be 200 kHz above 50 MHz, rather than 100 kHz. Our main argument is that we should allow the highest possible data rate in order to ensure the advancement of the state of the art. Propagation is better on lower frequencies than on UHF, and there is bandwidth available on 6 meters. This would be useful in rural areas where UHF propagation is hindered by foliage.

2. HSMM Networked Radios (The Hinternet) and the need for protection

Gerry Creager, N5JXS, states: "When the FCC ***WENT TO*** (emphasis added) the Part 15.ORG folk and solicited their help in New Orleans, they waived the power limitations on the WiFi element of the rules. In other words, they first sought another group (non-ham although a lot are licensed) and then waived the rules and asked them to do what hams used to do."

RECOMMENDATION: Please see Appendix A for Gerry's full report on the need for encryption on the Hinternet.

COMMENT: We currently recommend that all HSMM station computers (both connected to a radio and their associated network servers) be equipped with a firewall and an up-to-date anti-virus program. However, this is not considered to be adequate NETWORK protection by the network security professions within the working group. It is suggested that the Board consult with the Headquarters IT staff regarding what protection is currently being used to safeguard the ARRL intranet. Similar protection would be required to safeguard the Hinternet resources, too. Computer security requires, just as in the case of physical security, defense in depth. A firewall protects some aspects but not others. Dismissing encryption means usernames and challenge-response protocols are rendered in the clear and thus subject to interception and compromise. Hardware and IP address spoofing is now prevalent enough that the combination of interception of credentials and a little spoofing means your network is compromised.
We have to think of this as a system of security rather than any one specific part. We lose significant capabilities whenever we lose a security system element.

Respectfully submitted,

John Champa, K8OCL
ARRL Chairman
HSMM Working Group

Gerry Creager, N5JXS, Hinternet Architect reports on the need for encryption:

By way of introduction, I'm a staff researcher at Texas A&M University. These days, I manage a 35 terabyte data center for environmental and geophysical data. I'm a member of the Engineering Task Force for Internet2, the consortium of industry and universities researching and developing new internet systems, methods, protocols and hardware. I'm a member of Internet2's IPv6 (Internet Protocol Version 6) Working Group. I am the principal architect of the Virtual Network Engineering Laboratory at Texas A&M, which was funded by a grant from the National Science Foundation. Its purpose is to provide a facility to train network professionals without requiring their physical presence in the laboratory, and by using real network equipment instead of simulations. I am a member of the faculty of the Center for Information Assurance and Security at Texas A&M, which is funded and recognized as a Center of Excellence by the National Security Agency. We currently have four students enrolled in our certificate program, and the program undergoes biennial curriculum review by NSA.

I was first licensed as WN5THQ in 1967. I hold a General Class Amateur Radio license.

In the past, I was active while working at the Johnson Space Center, on the Shuttle Amateur Radio Experiment (SAREX), performing training, documentation, mission planning and mission control functions. During the STS-55 (Spacelab D2) mission with concurrent SAREX and SAFEX (European) Amateur operations on-orbit, I led the team that obtained permission to move SAREX operations to the Spacelab when we suffered a catastrophic failure of the antenna-coaxial cable system for SAREX. The import of this was that A) as an unplanned contingency operation it required mission management approval from Shuttle and Spacelab management and safety personnel, and B) it represented the fastest complete unplanned contingency operation in the history of Spacelab for a Shuttle system to utilize Spacelab systems. In other words, the technical and political challenges were daunting.

Finally, I am one of several who "tag-team" teach the graduate-level network security class here at Texas A&M. The nature of this class is that of "Black Hats" and "White Hats" or, attack and defend. We've found the best way to train defenders is to teach them how the attackers... hackers, crackers, bad guys... do their business. Unfortunately, in the world of computes and networking, the number of bad guys is high enough to make life difficult for the competent system administrators. Worse, the typical computer user is unsophisticated in protecting their own systems and assets, which means the administrators, have to protect whole networks because an attack on one host on a network, or the effective compromise of a single host, can adversely or even catastrophically affect an entire network of systems and potentially even a broader network area than that.

The questions we have to discuss are significant. Authentication and authorization are at the top but are not the sole issues.

Part 97 users are obligated under the Rules to prevent unauthorized use of Part 97 systems. The meaning of this, when applied to computer-based networks is that first, we must establish the identity of the individual requesting services and access; second, we must determine the level to which (s)he is allowed access to the full extent of the system; and third, how do we control access once the identity is established, and limit same to the capabilities level identified in (2) above. In the computer world, this remains an issue of significant study and experimentation. At Texas A&M, we have to go a step further on our wireless networks and attempt to maintain some degree of privacy, so we require all users to access the wireless network using a Virtual Private Network which is an encrypted system that "tunnels" or hides the content of the traffic within a packaging scheme that incorporates a crypto logically strong encoding to prevent unauthorized decoding and access.

Amateur operations using the 802.11 (WiFi) channels 1-6 encounter the same problem. Authentication and authorization remain key elements, especially since, on Channels 1-6, Part 97 is the primary user while Part 15 is secondary. Part 97 rules allow for more RF power output (100w vice 1w total system "ERP") and virtually no restrictions on antenna pattern or gain, unlike the system limits imposed on Part 15 WiFi. Thus, infrastructure created under Part 97 can legally, and should only, be used by licensed Amateurs if thy have taken advantage of the Rules with regard to Amateur use of this spectrum. Good practice, in this case, would require some minimum bar to admission be set.

HSMM have proposed such a minimum bar, but it is, in fact, so low, as to not represent any obstruction to access. We have proposed use of a WEP (Wireless Encryption Protocol) key that is published and available to Amateurs and the FCC. There are several problems with this approach.

1. The key is published. A cursory search using the Google search engine will reveal its contents and allow anyone to access any HSMM-supported system. However, this system was deemed appropriate by Chris Imlay, as not obscuring the contents of Amateur communications.
2. There exist in the public domain, a myriad of programs easily run on Windows, Linux and Mac laptops with wireless radios, as well as personal digital assistants (PDAs) running the Windows mobile platform or Linux, designed to capture packets seen on WiFi, decode their contents, and crack the WEP (and other such protocols) data. While the original exploit for WEP required some hundreds of hours and thousands of packets of data to perform this, today’s programs can operate in some

cases on as few as 100 packets and perform the cracking function in seconds. No longer is WEP, or its two newest rivals, considered safe.
3. WEP was originally based on weak encryption for simplicity, and then further compromised by implementation in how it handled serialization of the packets (sequential rather than disordered). This flaw allowed for critical "research" in breaking this encryption scheme. Later, crypto logically stronger schemes have proven little harder to exploit by the astute 16 year old interested in learning all he can about computers.

Single challenge-response ("password") based systems for authentication to a network have proven too easy to spoof and overtake to provide any realistic in restricting network access. Also, attempts to register the address of the Media Access Controller, or, the radio modem, are problematical because MAC addresses can be substituted by the hacker, allowing what the security community calls a "man in the middle" attack, where someone assumes the identity of a legitimate user and overtakes their session for their own ends. This scenario is neither far-fetched nor unproven. In fact, Man In The Middle is very easy to implement and we have seen it successfully used in our classes and security competitions a number of times using readily available scripts from the Internet.

Although not nearly so prevalent in the aging Amateur community, the concept of ubiquitous computing must also be considered. The majority of people who would be inclined to use HSMM would not do so on a computer solely dedicated to Amateur Radio and thus not holding personal data and identity information. In my household, I routinely have at least 4 computer systems networked together. I do employ stronger protection mechanisms than most, but then, considering my background, I'd be foolish not to. However, in my house, there are at least three Linux systems and a Windows system. I employ a personal firewall system, and it is updated with new attack profiles periodically. I also, however, employ a Windows system to keep the kids happy and try as I might, there is no good way to secure it while leaving it connected to the network.

I anticipate that the majority of Amateur Radio users will employ Windows systems. It has the greatest market penetration, it maintains the appearance of ease of use, and it plays the most popular games. The majority of the Amateur Radio software written has been written for Windows operating systems. Considering the degree of difficulty noted in securing Windows, we must approach security as a defense in depth.

Defense in depth means, simply, that you apply a number of layers of protection to the problem rather than depending on a single defensive mechanism to secure all your assets. Raising the bar to admission to the HSMM networks represents one element of a defense in depth. However, there's another issue to consider.

We have the flawed approach of a published security key, which we hope won't be found by the masses. This represents an approach to security known as "security through obscurity". Don't advertise it and they won't know it exists. Repeated experience demonstrates that Security Through Obscurity is fatally flawed. This is especially true in terms of a wireless system where its existence can be readily determined by passive means and where weak encryption can then be overcome. In other words, strong cryptographic means are required as an element of the in depth defense, as relying on someone not detecting the system is unlikely to succeed.

In terms of emergency communications (EmComm) requirements one of the things that has always offset the Amateur community from the rest has been that we used the systems day-to-day in normal operations, and no one had to suddenly re-familiarize themselves with new procedures. Once upon a time, when it wasn't important to hide the contents of almost every EmComm message... or for that matter, Health and Welfare in support of, i.e., the Red Cross... we could simply use the systems and procedures we had honed our skills on and proceed. As an extension of this thought, when I was active in AFMARS at the height of the Viet Nam conflict, our training routinely incorporated use of one-time pads and encoding to assure that we were trained in their use if needed.

The concept here is "Practice like you will play" or, in the parlance of the Army's Training and Doctrine Command (TRADOC), "Train like you fight". Amateur Radio must be prepared to do this, just as we had in the past, but now, the rules are different. If we're going to employ new systems, we need to prepare now to use them with strong encryption on a daily basis so that we're prepared to incorporate these tools when we're called upon to use them in an emergency. Also, it's important to demonstrate to the Emergency Managers and their communications designees that we're prepared to keep up with the times rather than reeling somewhere in the background. And today, we're reeling in the background.

HIPAA was originally envisioned to protect consumers from privacy invasions by insurance companies, in response to a problem either perceived or real, that information sharing in an inappropriate manner was ongoing. Its final form is truly frightening. The simplification of the 700-odd page bill, a document written by Congressional Staffers and the General Accounting Office, was some 1500 pages in length and I found it no easier to understand than the original bill. It took three long years of committee work to derive the Information Technology implementation rules for the Department of Health and Human Services, and the implementation has created a whole new industry designed to make a company, or an individual, HIPAA compliant. In all be the most emergent of cases, HIPAA covers what can an d cannot be discussed in unencrypted communications. I've heard cases in the Emergency Medical Services where paramedics are no longer allowed to provide any information that might provide any form of identifying information to the hospital in the course of emergency management of patient care. I've little doubt that, in the presence of something as trivial as a hurricane such as Katrina, HIPAA enforcement will ensue.

DHS has decreed that some communications can only be managed over encrypted links. They also have a stated interest in working with our Amateur assets, and in some cases, federalizing same. Once federalized, I suspect we're okay. Before that, however, if the need to pass the traffic exceeds the need to remain in compliance with Part 15, the operator in control has to make the call. Further, the American Red Cross has decreed that shelter lists of names of evacuees must be sent via secure means. They'd rather entrust these lists to cell phones than to Amateur communications, knowing the media will almost certainly monitor known Amateur nets for additional information but listening to all the cell channels would be challenging. I'm told that, in the event of loss of cell communications, they would not allow the lists to be handled by Amateur means because the lack of security is limiting.

Finally, Part 15 is not encumbered by limitations on encryption, and good engineering practice dictates its use. We are guided by a requirement to employ best practices, but then that option is currently removed from our capabilities, with respect to protecting systems and assets, and to providing needed services in times of emergency. Simply, we cannot encrypt while the secondary users of the spectrum can, and do. Parity and fairness dictate we be allowed the same degree of caution the unlicensed segment is afforded.

My particular piece of HSMM is "infrastructure", or, links from point to point, and creating the underlying network on which the HSMM activities can proceed. The network I've envisioned and spoken on often, is content agnostic. However, access to that network requires care and caution, and at this time, the Rules do not allow these capabilities.

The basis for refusing encryption in the Amateur service is an international fear that Amateur communications will unfairly compete with common carriers. At least in the United States, it's now unlikely to happen. In some developing countries, this may still be a consideration, but I do not see how that should affect activities in this country. I strongly believe that we need to undertake a rules change to allow encryption in the Amateur Service at all frequencies for networks where access to computer systems and to Part 97 controlled RF networking assets are employed.