SECURITY & DATA INTEGRITY
ON A
MODERN AMATEUR RADIO NETWORK

By
Paul J. Toth – NA4AR
Emergency Communications Specialist
ARRL HSMM Working Group

Amended 6/29/2004

EXECUTIVE SUMMARY

This document has been prepared by the ARRL High Speed Multimedia & Networking Working Group (HSMM) to highlight a growing need for regulatory change governing high speed, wireless data stations operating in the Amateur Radio Service. The HSMM respectfully requests the support of the ARRL Board of Directors for development and filing of a Notice of Proposed Rulemaking (NPRM) ***permitting the use of encryption and strong security protocols on domestic transmissions above 50 MHz***.

Part 97 has, for decades, required that all Amateur Radio Service communications be conducted "in the clear". ITU regulations and treaties, to which the United States is a signatory, prohibited the use of ciphers and schemes designed to conceal the meaning of transmitted communications. However, an amendment made to Article 25.2A (1A) at the 2003 World radio Conference no longer specifically prohibits the use of encryption and other strong security measures on transmissions between Amateur Radio stations within the same jurisdiction.

Several recent events are driving the need for stronger station access and content security. These include:

- The need to prevent access to Amateur Radio stations by millions of unlicensed commercial and non-commercial users operating under Part 15 of the FCC's rules.
- The need for Amateur Radio operators providing emergency communications services to observe significant changes in security and privacy regulations.
- The continuing threat to Homeland Security since the 9/11 Attacks have caused numerous Federal, State and local agencies to mandating more secure communications.

Amateur Radio Service has shared spectrum in harmony with other FCC licensed radio services, primarily non-commercial government operators. However, commercial, for profit traffic and messages that are prohibited under Part 97, are now routinely transmitted by millions of unlicensed businesses and individuals on bands previously allocated for non-commercial use. Unlike Part 97 operators, these non-licensed users are free to employ strong industry-standard security protocols to prohibit unauthorized access and to protect the integrity of the transmitted content.

The availability of these unlicensed devices, coupled with an armada of sophisticated software tools has severely compromised Amateur Radio operations on numerous bands. Most notable are bands above 902 MHz, including those allocations where the Amateur Radio Service is designated the Primary Service. At the same time, Hams are prohibited from securing their transmitters, the computers and other technology connected to the transmitters and the information those systems store from unwanted intruders. It could be said that this has left licensed Amateur Radio operators swimming totally unprotected amongst a sea of hungry sharks.

This new landscape seriously compromises the relevance of Amateur Radio communications in our Twenty-first Century society. As laws governing society and

information mandate more privacy and security, the Amateur Radio Service finds itself hamstrung by outdated and outmoded regulations. The existing regulations are in direct conflict with policy changes and regulations now being used by many disaster responses organizations previously served well by Amateur Radio Service licensees. The events of 9/11 have changed the landscape for all communications, particularly emergency and disaster-related transmissions. Without the legal authority to employ strong security protocols, the Amateur Radio Service will be out in the cold, unable to serve and fulfill one of our prime mandates. These prohibitions will also serve to stifle continuing technological innovation, a cornerstone of Amateur Radio.

The HSMM Working Group believes a solution to this dilemma is achievable. Changes to international regulations governing Amateur Radio communications permit the local governing authority, the FCC, to legalize the use of encryption and strong security protocols on domestic transmissions. Further, the FCC has publicly stated that a policy allowing it to easily monitor Amateur Radio Service transmissions is no longer enforced on frequencies above 50 MHz.

Thus, he HSMM Working Group respectfully asks the ARRL Board of Directors for their support of this needed regulatory change and urges the Board to support the development and filing of a Notice of Proposed Rulemaking (NPRM) ***permitting the use of encryption and strong security protocols on domestic transmissions above 50 MHz***.

KEY POINTS

The HSMM Working Group was established by the ARRL Board of Directors to further develop high-speed digital operations under Part 97. Our work has focused on several key areas, including:

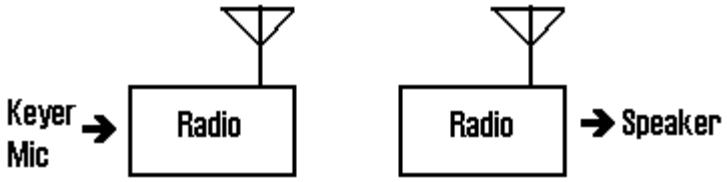
- FREQUENCY ALLOCATIONS best suited for Broadband Operations
  Amateur radio has several allocations above 420 MHz that are well suited for broadband digital operations. These include: 420-450 MHz, 902-928 MHz, 1240-1300 MHz, 2390-2450 MHz, 3300-3500 MHz, 5650-5925 MHz, and 10.0-10.5 GHz
- BAND SHARING with Other LICENSED Services
  Several of the bands denoted above are shared with non-commercial licensed radio services, primarily the Federal government. While the opportunity for interference exists, we do not see this as a major issue.
- BAND SHARING with UNLICENSED Operators
  In recent years, the FCC has encouraged unlicensed commercial and non-commercial utilization of these bands. In fact, WRC-03 made a global, PRIMARY allocation of 5150-5350 MHz and 5470-5725 MHz for "wireless access systems, including RLANS". The development and mass marketing of low cost, low power Part 15 transmitters has resulted in millions of these devices operating on the 902-928 MHz, 2400-2450 MHz and 5650-5925 MHz bands. This significantly increases the probability of illegal use of unsecured Amateur Radio transmitters by Part 15 operators and other security breaches that can lead to loss of data and the compromising of attached ancillary systems.
- STATION SECURITY
  Part 97 requires Amateur Radio Service licensees to prevent unlicensed operators from access to their stations. However, Part 97 prohibits licensees from using the industry-standard 802.1x and other security measures found on low cost 802.11(a)(b)(g) transceivers. This leaves licensed stations open to unwanted and illegal access by unlicensed operators, many transmitting commercial content, jeopardizing the licensee's privileges.
- DATA INTEGRITY
  Part 97 prohibits the use of ciphers and symbols to hide the meaning of transmitted message content. The continuing threat to Homeland Security following 9/11 coupled with the enactment of stringent privacy policies and laws, like HIPAA, prevent Amateur Radio operators from providing needs communications services to many disaster responses agencies and organizations previously served. This new landscape seriously compromises the relevance of "open" Amateur Radio communications in our information-driven 21st Century society. This will have a chilling impact on the recruitment of new licensees, on

future innovation and discovery in the wireless realm and on the ability of the Amateur Radio Service to provide emergency communications services as needed.

The submission and enactment of a Notice of Proposed Rulemaking (NPRM) permitting the use of strong security and content encryption will enable Amateur Radio operators to abide by existing regulations prohibiting unlicensed use of station facilities. It will, further, re-affirm the Amateur Radio Service as a relevant and responsive part of the domestic communications fabric.

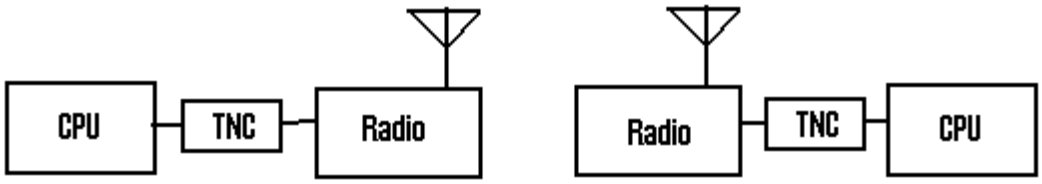
THE CHALLENGES

If someone requested a diagram of a "traditional" Amateur Radio communications system, it would probably look like the diagram below. One operator, using a Morse Code keyer or a microphone sends a message on some assigned frequency to another operator who receives the message with a similar radio equipped with a speaker.



It has been seventy years since the Congress and the Communications Act of 1934 formalized the Amateur Radio Service. While this basic communications model is still a valid representation of how Radio Amateurs can communicate, the Federal Communications Commission and advancements in communications technology now enable us to communicate in many other ways.

For example, the advent of the personal computer in the 1980's led to Packet Radio, where a computer connected to a Terminal Node Controller and a radio allowed operators to send text to one another, keyboard to keyboard in real time or by transferring files located on a disk.



Packet Radio

The security of the information and the computer technology connected to the Amateur Radio transceiver was not in question because of the relative simplicity of the systems and the lack of connectivity to other computers.

The invention of Ethernet, a technology now widely used to link computers and other information devices together in a network, further expanded our ability to communicate over wired media with these devices. Computer networks are now common- place in business and in many homes.

More recently, in the mid-1990s, an Information Revolution was fueled when computers of various shapes, sizes, Operating Systems and purposes connected to the Internet. A creation of DARPA in the late 1960s, the Internet had been used primarily for research by various

colleges and universities as well as by the Federal government. The commercialization of the Internet at the end of the Twentieth Century was responsible for an exponential proliferation of digital information systems, capable of reaching halfway around the world and providing access to information in milliseconds. Schools, hospitals, businesses large and small and millions of home worldwide are now linked together via the Internet. The potential for significant benefit from this degree of connectedness is almost boundless; however, the potential for great harm from providing access to malicious individuals is also increased.

As computers got smaller, faster, capable of processing many different kinds of information, a growing clamor arose for low cost, unlicensed wireless connectivity. The groundwork for this use of the radio spectrum had been laid by the FCC with the allocation of several unlicensed bands under Part 15. Most of the early Part 15 broadband devices were slow and expensive. But with demand in the marketplace exploding, coupled with the legalization of DSSS and OFDN, low cost Part 15 devices became plentiful.

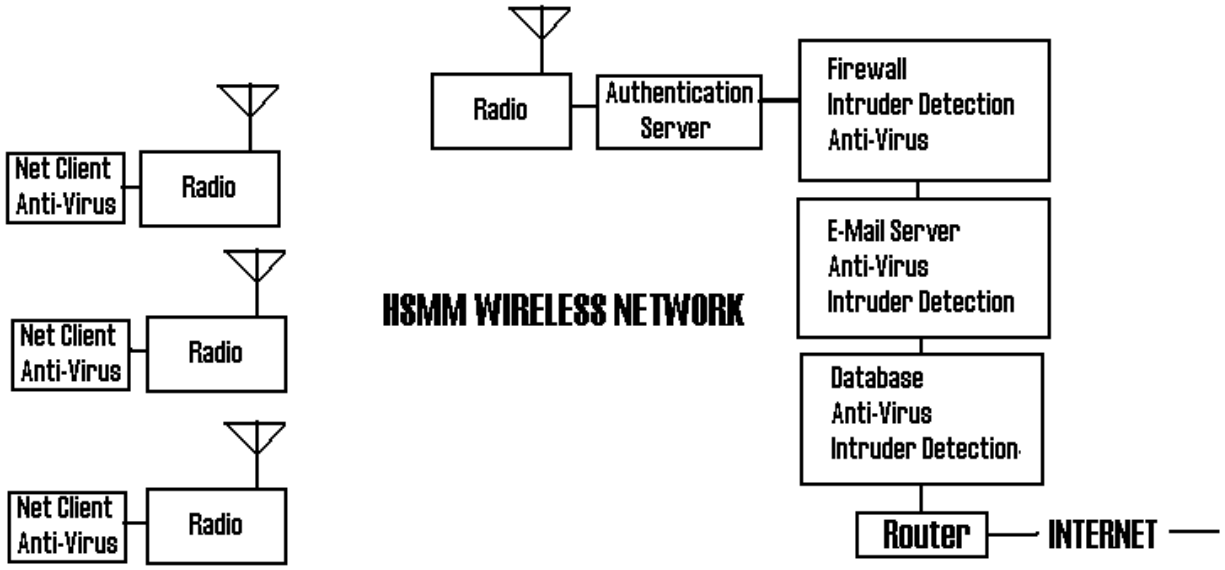
Part 15 transceivers operate with low power output and other restrictions that limit their overall range. Manufacturer adoption of several IEEE standards, including 802.11(a)(b)(g) has empowered millions of unlicensed individuals, businesses and government organizations to get on the air. In some cases, remote offices are now connected to the main office using these radio transceivers, eliminating costly data circuits leased from the local phone company. Much of this activity uses spectrum that overlays the Amateur Radio Service allocations at 902 MHz, 2.4 GHz and 5.7 GHz. Further systems may include the use of Part 15 frequencies that reside within the Amateur Radio Service bands between 1240 MHz-1300 MHz and 3300 MHz-3500 MHz.

Amateur Radio operators have successfully shared spectrum with other licensed, non-commercial Radio Service users, including the government. These other stations operate within rules that mirror Part 97. Stations are required to identify themselves. Their operating modes are defined and emissions quantified.

The impact of the FCC's decision to permit unlicensed, broadband radio transceivers to operate under Part 15 on frequencies shared with the Amateur Radio Service has dramatically changed the landscape for Part 97 users. Part 15 hotspots (Wireless Access Points) are commonplace. Signal saturation from unlicensed users is an increasing problem, particularly in large urban areas.

Part 15 rules lack compatibility with Part 97 in a number of other significant ways. Part 15 rules do not require station identification. Part 15 operators are free to convey commercial traffic in which they have a pecuniary interest. There are no prohibitions on the use of encryption and other security measures to protect the many computers, disk drives and information stores connected to these radios. These strong security tools can also be freely used (and are commonplace) to secure the authentication process as authorized users attempt to gain wireless access to the information resources, including the Internet, connected to these Part 15 transceivers.

A typical Part 15 wireless network, operating with IEEE standard 802.11a/b/g radio technology may look like this.



It is a common and best industry practice for User Authentication and passwords to be transmitted using strong security protocols. It is also a common and best industry practice for messages and other data to be "tunneled" using Virtual Private Networking, sets of protocols that purposely make it extremely difficult for data theft by radio signal interception to be successful. As you can easily see, this is significantly more complex that the Communications Model shown at the beginning of the document.

If Radio Amateurs are to exercise the operating privileges they have been granted on several assigned bands now openly used by non-licensed Part 15 operators, we, too, will need the freedom to utilize the same security tools and protocols to keep these unlicensed users from access our stations. Computer programs, like NetStumbler, permit anyone with a WLAN transceiver to eavesdrop and intercept broadband data signals and decipher their content. This has led to numerous computers and networks attached to these wireless transceivers being breached, compromised and ransacked. Several State and Federal courts have ruled it is the responsibility of the wireless transceiver operator to prevent would be intruders from breaching these transceivers and the information resources attached to them. Without the use of Authentication servers and protocols, firewalls, Virtual Private Networks, Secure Socket Layers and other Information Management tools, these radio transceivers and the other technology and data connected to them are indefensible to attack.

REMEDIES

Radio Amateurs are REQUIRED to SECURE their transmitters and prevent access from anyone not holding a valid Technician Class or higher Amateur Radio license [97.5(a)]. Because the industry standard tools needed to accomplish this are prohibited under Part 97, this requirement has created a virtual impossibility.

Further, laws and regulations governing information security and release have changed dramatically as concern over personal privacy has increased. The HIPAA laws and private and governmental Privacy Policies have raised the bar on the transmission of many kinds of information and personal data. This severely limits the ability to the 21st century Radio Amateur to provide critical, relevant communications service and conduits during and after real emergencies.

IEEE standard 802.1x exists to provide a roadmap and standard for station authentication and access to broadband, wireless data systems. Other industry-standard protocols, including but not limited to WEP, EAP and LEAP are commonly used outside the Amateur Radio Service to provide secure station and user authentication.

Licensees in the Amateur Radio Service need to be free to utilize these and other industry-standard security and authentication tools to protect the integrity of their stations, particularly on bands shared with Part 15 operators. Amateur Radio Service licensees should also be allowed to protect the security and the integrity of the information their stations are conveying. Use of PPTP, Secure Socket Layer (SSL), Secure Shell (SSH), Virtual Private Networking and other standard protocols and tools are routinely used to convey information in a secure manner on wired and wireless links. Amateur Radio operators should be permitted to use these tools as they represent "good engineering practices" in modern data and information management. Information conveyed in the clear is no longer an option for many essential service providers who rely on Amateur Radio operators when normal communications systems are not available.

These measures will enable Amateur Radio Service licensees to successfully co-exist with operators governed by other rules and operate in accordance within other Part 97's specifications, resulting in a minimum of interference and security concerns. They will allow the development of Amateur Radio infrastructure capable of yielding new, innovative capabilities and methods, proving out those capabilities and methods under a variety of operating conditions, allowing licensees to communicate in ways never before possible. This will lay a solid foundation for Amateur Radio Service licensees nationwide to use our assigned spectrum and license privileges to provide essential, relevant emergency communications services to our communities when they need us the most.

The popularization of the Internet has fueled an information-driven society. Add to this a policy of spectrum sharing and the events of 9/11/2001. The realities of the 21st Century present a difficult and challenging operating landscape for the Amateur Radio Service. It is time to modernize Part 97 to reflect these changes. This will allow U.S. Radio Amateurs to continue a proud tradition of innovation and service when it is needed most.

ACKNOWLEDGMENTS

This document was developed with significant input and expertise from members of the HSMM Working Group, including:

John Champa-K8OCL
Gerry Greager-N5JXS
Walt Dubose-K5YFW
Dave Anderson-KG4YZY
Dave Stubbs-VA3BHF
Ron Olexa – KA3JIJ
Joe Cupano-NE2Z
Jeff King – WB8WKA
Carl R. Stevenson-WK3C
Howard Huntington-K9KM