Authentication for Amateur Radio

Why We Need It and How To Implement It

Bryan Hoyer
KG6GEU

NW Digital Radio

What is Authentication?

- The Process of *Reasonably* Verifying:
  - Who Sent the Message
  - When it was Written
  - The Message's Integrity

NW Digital Radio

Authentication...

... is not Encryption

- How do we Know?
  - The Message is Sent in the Clear, the Meaning is Not Obscured
  - Encryption is Subject to Export Restrictions, Authentication is Not

NW Digital Radio

Why Do We Need It?

- All Digital Comms use USERNAME/ PASSWORD, Except Amateur Radio WHY?
- Are Hams any Better than the General Population?
  - Access Control?
  - Malicious Behavior?

NW Digital Radio

Where Do We Need It

- Health Safety
  - Traceability
- EMCOMM
  - Moving Men and Material
- Rig Control
  - You have to ask?

NW Digital Radio

What Does It Cost?

- Some Processing on Both Ends
- Some Additional Bytes in the Message
- The *Application* Determines How Much

NW Digital Radio

Is It Really Secure?

KEY (BITS)	YEARS	KDOLLARS
50	36	$31
60	36,559	$32,026
70	37,436,315	$32,794,212
80	38,334,786,264	$33,581,272,767

1GHz CPU Computing SHA-1 in 1000 Cycles
CPU Cost $0.10/Hr
Best Collision Attacks are currently 2^69 for 80 Bits
Collision Attacks do not affect HMAC

NW Digital Radio

Email Implementation

- Email Over Radio is Still Email
  - Let the Mail Client Handle It!

NW Digital Radio

Digital Signature DSS

- Obtain a Certificate
  - Certificate Authority
  - Self Signed
- Use S/MIME
  - Overhead 3-5Kbytes/Message
- smime.PS7 File Attached

NW Digital Radio

GPG Mail Client

- Append Public Key to Message
  - Overhead ~500Bytes/Message
  - Anyone Can Authenticate
- Or Use Fingerprint
  - 70 Bytes
  - Must Have Key Saved Locally

NW Digital Radio

What About APRS?

- Maximum Size for UI Frame
- AX.25 256 Byte Info Field
- APRS Message 67 Characters

NW Digital Radio

HMAC

- Hash-based Message Authentication Code
- Secret Key 160 - 256 Bits
- Digest of 20 - 32 Bytes
  - Truncate to 10 - 16 Bytes
  - Base91 Encode to 14 - 22 Bytes for APRS
  - Versus 6 Bytes for Message Number

NW Digital Radio

Sample Message

- APRS Message 47 Characters Max
- AX.25 UI Frame 230 Characters Max
- Include Timestamp for Freshness
- APRS Format
- Terminate with | character

:KG6GEU-00:@MDHM Maximum *APRS* message, with an HMAC appended |kySfdKnB9^MG

NW Digital Radio

Deployment

- A Club or other Group shares a single Key via a Secure Meeting
- Group Members use HMAC to send Authenticated Messages
- EVERYONE can Read ALL Messages
- Group Members can Authenticate Received Messages

NW Digital Radio

Rig Control Today

- Pick an Weird Frequency
- Add a Tone
- DTMF Control
  - Use OTA Access Code
- Hope NoOne is Listening

NW Digital Radio

DTMK ™ Control

- "Don't Touch My Knob"
  - Radio Authenticates Commands Sent as Plain Text Messages

:KG6GEU-03:03/31/12 17:09:11 QSY 443.250 |5q&`_b\mSWO)

NW Digital Radio

EMCOMM CallOut

- In the Event of a Communications Emergency Dispatch Needs to Contact Amateur Radio Personnel
- Communications are Disrupted
- Amateur Radio is Not Legally Available

NW Digital Radio

Message Forwarding System

§97.219 Message forwarding system.

=

(a) Any amateur station may participate in a message forwarding system, subject to the privileges of the class of operator license held.

(b) For stations participating in a message forwarding system, the control operator of the station originating a message is primarily accountable for any violation of the rules in this Part contained in the message.

(c) Except as noted in paragraph (d) of this section, for stations participating in a message forwarding system, the control operators of forwarding stations that retransmit inadvertently communications that violate the rules in this Part are not accountable for the violative communications. They are, however, responsible for discontinuing such communications once they become aware of their presence.

(d) For stations participating in a message forwarding system, the control operator of the first forwarding station must:

(1) Authenticate the identity of the station from which it accepts communication on behalf of the system; or

(2) Accept accountability for any violation of the rules in this Part contained in messages it retransmits to the system.

NW Digital Radio

Third Party Communications

§97.115 Third party communications.

-

(a) An amateur station may transmit messages for a third party to:

(1) Any station within the jurisdiction of the United States.

(2) Any station within the jurisdiction of any foreign government when transmitting emergency or disaster relief communications and any station within the jurisdiction of any foreign government whose administration has made arrangements with the United States to allow amateur stations to be used for transmitting international communications on behalf of third parties. No station shall transmit messages for a third party to any station within the jurisdiction of any foreign government whose administration has not made such an arrangement. This prohibition does not apply to a message for any third party who is eligible to be a control operator of the station.

(b) The third party may participate in stating the message where:

(1) The control operator is present at the control point and is continuously monitoring and supervising the third party's participation; and

(2) The third party is not a prior amateur service licensee whose license was revoked or not renewed after hearing and re-licensing has not taken place; suspended for less than the balance of the license term and the suspension is still in effect; suspended for the balance of the license term and re-licensing has not taken place; or surrendered for cancellation following notice of revocation, suspension or monetary forfeiture proceedings. The third party may not be the subject of a cease and desist order which relates to amateur service operation and which is still in effect.

(c) No station may transmit third party communications while being automatically controlled except a station transmitting a RTTY or data emission.

NW Digital Radio

Operation HogCall ™

- Dispatch Composes a Message via a Web Form on their LAN
  - Form Controls Content 97.219 d(2)
- Radio Transmits Bulletin Indicating it Has Traffic (Telemetry)
- Responders Check-In and Receive Message

NW Digital Radio