NW Digital Radio

TELECOMMAND:
Using Authenticated APRS Messaging for Remote Control

Bryan Hoyer
K7UDR
“Necessity is the Mother of Invention”

Author Unknown
Rig Control Today

- Pick a Weird Frequency
- Add a Tone
- DTMF Control
- Use OTA Access Code
- Hope No One is Listening
- “Security by Obscurity”
DTMK Control

- "Don't Touch My Knob"
- Radio Authenticates Commands
- Sent as APRS Messages
- Signed with HMAC

:K7UDR-03: QSY 443.250 \S5H%b
What is Authentication?

- The Process of Reasonably Verifying:
  - WHO Sent the Message
  - WHEN it was Sent
  - That the Message has not been ALTERED
Authentication...

... is not Encryption

- The Message is Sent in the Clear, the Meaning is Not Obscured
- BTW Encryption is LEGAL in Amateur Radio
Why Do We Need It?

- All Digital Comms have Security Issues
- Are Hams any Better than the General Population?
- Access Control?
- Friendly Fire?
- Malicious Behavior?
Where Do We Need It

- EMCOMM
- Moving Personnel and Material
- Rig Control
- You have to ask?
- Why not just use it?
What Does It Cost?

- Some Processing on Both Ends
- Some Additional Bytes in the Message
- The Application Determines How Many
  "Just Enough Authentication"
YAAC

• Yet Another APRS Client
• Andrew Pavlin KA2DDO
• Written in Java (Platform Independent)
• Open Source
• Under Active Development
HMAC

- Hash Based Message Authentication Code
- Public or Private Key 128 Bits 16 Bytes
- MD5 Creates Digest of 16 Bytes
- Salt with UNIX Time to the Minute
- Base 85 Encode = 20 Characters
Send as Many as You Need

• “There once was a Ham from Nantucket”
• T=0 B13es2aH__8S4T?`Cm`l
• T=1 Ob"GY>Ibqs3il#PUCu:&
• T=2 :M(DF#Zb))`nZ\%oR$!u
• Truncate and Transmit!
# Just Enough Security

<table>
<thead>
<tr>
<th>Number of Unique Codes</th>
<th>Time to Sneak One Thru!</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>85</td>
</tr>
<tr>
<td>1</td>
<td>85</td>
</tr>
<tr>
<td>2</td>
<td>7,225</td>
</tr>
<tr>
<td>PIN4</td>
<td>10,000</td>
</tr>
<tr>
<td>PIN6</td>
<td>1,000,000</td>
</tr>
<tr>
<td>4</td>
<td>52,200,625</td>
</tr>
<tr>
<td>6</td>
<td>377,149,515,625</td>
</tr>
<tr>
<td>8</td>
<td>2,724,905,250,390,620</td>
</tr>
<tr>
<td>10</td>
<td>19,687,440,434,072,300,000</td>
</tr>
<tr>
<td>20</td>
<td>387,595,310,845,144,000,000,000,000,000,000,000,000,000,000,000,000,000</td>
</tr>
</tbody>
</table>

10 Minimum recommend size per RFC 2104
Private Key Deployment

- A Club or other Group shares a Private Key (20 Characters) via a Secure Channel
- Group Members use HMAC + Key + Time to Sign Messages
- EVERYONE CAN READ ALL MESSAGES
- Group Members can Authenticate Received Messages
Public Key Deployment

- A Key Pair is Generated
- The Private Key is shared as before and used to sign messages
- The Public Key is Posted on a Website
- Anyone can Authenticate the Message Using the Public Key
- LOTW Logbook of the World
Does Anyone Really Know What Time It is?

- UNIX Time
- Number of Seconds since the EPOCH
  - 00:00:00 UTC January 1st 1970
  - 32 bit number
  - Rolls over on XXX

NW Digital Radio
Ways to Get the Time

• From the Internet NTP
• From a GPS Receiver
• From a local RTC
• What about Drift?
APRS Time Server

- Sends Time Code Periodically as Beacon
- Identifies its source GPS or NTP
- Sends Authenticated Message
- Uses Public Key Technology
- Receiver adds Public Key
- Trusted Time Server
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
HogCall

- Dispatch Composes a Message via a Web Form on their LAN
- Form Controls Content
- Radio Transmits Bulletin Indicating it Has Traffic (Telemetry)
- Responders Check-In and Retrieve Message
§97.219 Message forwarding system.

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

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

§97.115 Third party communications.

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