Authenticating Friend or Foe

14 January 2021

Statement of Purpose: Address authentication best practices and guidance for determining that another station is who they claim to be.

Intent: Provide AmRRON Operators with an understanding of various authentication tools and practices, and the varying degrees of levels of authentication, including their limitations.

General Guidance:

Not all authentication is a guarantee that the person you're communicating with is who he or she says they are. However, there are ways that you can increase the odds and minimize the risk. If done properly, you *can* be absolutely certain!

The best way to know if the person you are talking to is who he says he is, is to KNOW him (his voice, his nuances, and his mannerisms). This kind of trust is built over TIME. This is precisely why we have urged radio operators to join years in advance of an emergency, and to be engaged with one another. AmRRON members who have invested time with each other have developed friendships, trust, and personal authentication plans between themselves over the course of time.

Newcomers are at a disadvantage, but there are still steps one can take to minimize risk and have higher confidence that the people you're communicating with and the information being passed is genuine and authentic.

1. (Medium/Low Security) The AmRRON Signals Operating

Instructions has a small section covering authentication in the form of a 10-letter word. That is contained on Page 97 (or Section 10.5.3), including an explanation of how to use it.
AmRRON Corps operators also have an expanded authentication table in the Corps Annex, exclusive to the AmRRON Corps SOI, Version 4.2(C). This is typically used by one AmRRON station to authenticate another.
IMPORTANT: successfully authenticating another station using this method does not distinguish between friend or foe. It merely means the other station also has a copy of the SOI. This is intended to increase the *likelihood* that you are communicating with another AmRRON operator, and hence, and increased likelihood that it is a

Authenticating Friend or Foe

14 January 2021

like-minded (patriot/preparedness minded) party.

2. (Medium/Moderately High Security) Beginning January 12, 2021, all 'official' digital traffic sent from AmRRON National will be authenticated with a Checksum Hash. Specifically, the reports and forms will be saved as .txt files or .k2s (Custom flmsg forms), hashed, and sent using FEC (Forward Error Correcting) modes, such as FLAMP, to ensure the integrity of the file.
IF the file is passed on this way, it will minimize corruption of the file and increase the chances of a successful checksum verification.

Regional NCSs who generate traffic for their regional nets may also hash their files and send them securely to AmRRON National where the has can be displayed at AmRRON.com. NCS should let you know during the net.

To learn more about Checksum hashing, see the white paper linked below:

https://amrron.com/2019/03/13/white-paper-hashing-files-with-checksum-utilities-tamper-detection/

Special note: Sometimes data gets corrupted during transmission, or a operator will inadvertently change something in the file, including the file name. These things do occur and it will cause a checksum file hash to fail verification. This does not mean it was done with malicious. It simply means something has changed from what was contained in the original file, even something as simple and small as a (.) period.

3. (More Secure) You may begin seeing 'Authentication:...' followed by letters, numbers, or a combination of both. This is an authentication process developed between two or more stations in advance. Unless you have been specifically notified and coordinated with by someone, this would not be something you could make use of and does not pertain to you.
Additional note: Authentication is NOT encryption.

Authenticating Friend or Foe

14 January 2021

4. (Most Secure) All operators are strongly encouraged to coordinate with the other operators directly which you communicate with on a regular basis, and exchange some method of authentication between yourselves.
This takes time, but is very important when practical. Authentication information should be exchanged face to face, or by using encrypted methods such as pgp encrypted email, or Protonmail (based in Switzerland, they offer free encrypted email accounts).

=======

AmRRON staff and senior members such as Net Control Stations and others have long-established authentication procedures between themselves. If you receive or see radio traffic that seem suspicious or outlandish, or otherwise doesn't seem to reflect AmRRON's mission statement, ideals, values, and common practices, it it highly likely that what you see going over the airwaves isn't authentic AmRRON traffic.

For numerous reasons, whether out of spite, boredom, or maliciousness, there are some who might try to pass false radio traffic with the intent of causing confusion and misinformation, or of painting AmRRON and its members in a negative or even 'extremist' light.
If you see this kind of traffic over the airwaves, first attempt to authenticate the traffic with the sender to be sure it's real AmRRON traffic. If you're not able to authenticate, then get hold of other AmRRON operators using the Z-Net, the forum, or directly over the air, and inquire.
Hopefully you're getting familiar with some of the more seasoned, experienced AmRRON operators as you spend more time on the air. Chances are very high they'll be able to let you know if traffic you're seeing is authentic, or they'll know who to get hold of to find out.

And if you see traffic or activity on the AmRRON nets which seems suspicious, false, or malicious, report the traffic directly to johnjacob at amrron.com and nets at amrron.com.