AAAAA – Assembly, Acquisition, Access, Authentication, & Authorization Protocol for Phase 4 Ground (P4G) – A Digital Amateur Radio Satellite System

Paul Williamson, Tilak Marupilla, Michelle Thompson
Open Research Institute, Inc.

Abstract

Open Research Institute's Phase Four Ground (P4G) project [1] has defined a digital communications system based on many single-user FDMA channels of digital uplink data and a single DVB-S2/X downlink channel. Experience with satellite communications systems has revealed a variety of problems, which could hamper the safe functioning and interrupt the communication of the satellite to other users.

This poster covers a Threat model, AAAAA acronym & finally proposes a Crypto Handshake process to mitigate the threats, using LoTW (Logbook of The World) public key cryptography certificates [2] to authenticate a ground station, generate a secret key on both sides using ECDH Diffie-Hellman [3], and finally generate authentication tokens using the secret key generated (using a TOTP-based mechanism). Further some thoughts on Jamming mitigation are also discussed.

Threat Model

Generic Threat Model:

- Users with no identity or impersonated identity
- Message/Payload Integrity from modification
- Replay attacks
- Jamming (Intentional/Unintentional)
- Denial of service attack

AAAAA

Assembly
When a new ground station is constructed, it must be configured to operate with the system, including the provisioning of any cryptographic secrets and certificates that may be required for participation in the security aspects of the system.

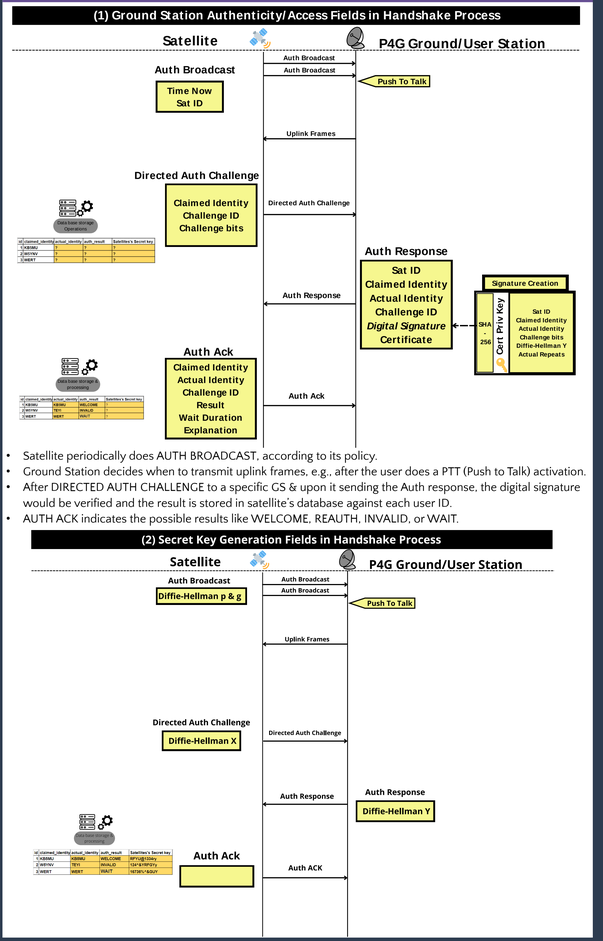
Acquisition
When a ground station is turned on, it faces the problems of acquiring the downlink signal from the payload, and initializing itself to work with whatever operating state the system happens to be in.

Access
When a ground station wishes to transmit through the system, it must go through special procedures to make its presence known to the payload and begin to communicate.

Authentication
Whenever a ground station is participating in communications through the system, the payload has the option to request that the ground station prove that its claimed identity (its callsign) is authentic. Such requests would be driven by system policy, and might vary from payload to payload, from time to time, and from user to user, all driven by system policies.

Authorization
The purpose of authentication is to enable the payload to enforce an authorization policy. That is, the payload may choose to impose limits on certain ground stations or even block them entirely from using the system.
Our AAAAA design goal is to make the system as painless to use and robust as possible, while strongly encouraging that systems be freely available to all licensed amateurs. By providing the mechanisms to defenestrate a few miscreants when necessary, we hope to make the system a joy to use for the vast majority of cooperative radio amateurs. Perhaps the very existence of the mechanisms will be enough to discourage bad behavior.

One Protocol Exchange, Three Functions



- Satellite periodically does AUTH BROADCAST, according to its policy.
- Ground Station decides when to transmit uplink frames, e.g., after the user does a PTT (Push to Talk) activation.
- After DIRECTED AUTH CHALLENGE to a specific GS & upon it sending the Auth response, the digital signature would be verified and the result is stored in satellite's database against each user ID.
- AUTH ACK indicates the possible results like WELCOME, REAUTH, INVALID, or WAIT.

Function 2 – Secret Key Generation using (Elliptic Curve) Diffie-Hellman:
Auth Broadcast:

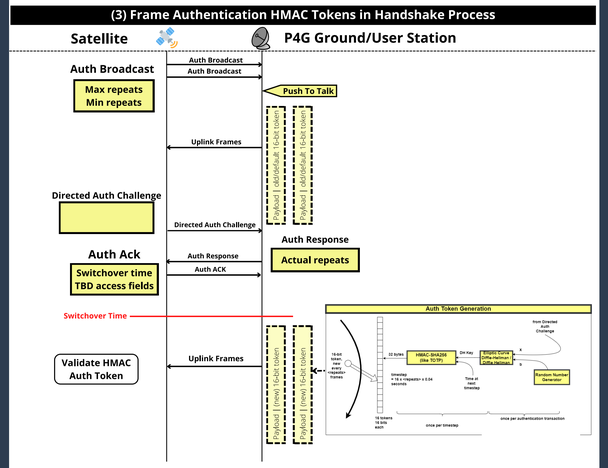
- Commonly agreed prime and generator values are used by both parties to compute their respective Public & Secret keys in a two-step process

$X = G^a \bmod p \qquad Y = G^b \bmod p$

Directed Auth Challenge & Auth Response

- Satellite shares its Public key X and GS user will share its Public key Y (not the private a & b values) in Directed Auth Challenge and Auth Response messages, respectively.
- Now both parties can compute the (identical) shared secret key. Ground station uses it to generate tokens for uplink frames, and the satellite uses it to verify those tokens..

$(Y^a) \bmod p \quad == \quad (X^b) \bmod p$



Function 3 – Continuous sender identity check by using a TOTP-like HMAC Token in every frame:

- After **AUTH RESPONSE** message, both Satellite & GS have the same secret key.
- Ground station will use a mechanism similar to TOTP (Time-based One-Time Password) [4] to generate small 16-bit authentication tokens included in each frame.
- Computation load can be moderated by repeating each token in several frames, as negotiated in the handshake within parameters set by the satellite in the Auth Broadcast message.

Jamming

No cryptographic authentication scheme can stop brute-force attacks from interfering with communications through the system. If a jammer is able to continuously overwhelm the entire uplink band with excessive power, the system will be rendered useless, but the jammer will also be relatively easy to track down.

Uplink Frequency Diversity
The uplink consists of many relatively narrowband single-user channels. An individual narrowband jammer with enough power can interfere with at most one of these channels at a time. In order to significantly reduce the system capacity, the jammer would need to interfere with many of the uplink channels, which multiplies the interfering power needed and the complexity of the jammer's equipment.

Targeted Jamming
If a malicious uplink jammer with limited equipment intends to interfere with a particular uplink user, it would need to know which uplink channel the targeted user is transmitting on. If the jammer is physically adjacent to the target, it can simply listen on the uplink, and we can't do much about that. If not, the jammer can only go by what is heard on the downlink. More work is needed to define a procedure that allows the authorized uplink stations to choose interference-free channels without also helping a malicious jammer to target the used uplinks.

Conclusion

Open Research Institute, Inc. (ORI) is a non-profit research and development organization which provides all of its work to the general public under the principles of Open Source and Open Access to Research. ORI's Phase 4 Ground Station and Phase 4 Space projects are working to bring advanced digital communication techniques to the amateur satellite service, in the belief that digital systems offer many advantages over simpler analog systems. Some of these advantages take the form of effective protections against patterns of abuse that are difficult or impossible to defend against in analog systems. The work shown here is an attempt to use common cryptographic techniques to realize some of these protections, while staying entirely within the regulatory framework of amateur radio, which currently prohibits the use of encryption when it is intended to obscure the meaning of communications.

This is an early design, and the volunteers who have come up with it are not cryptography experts (yet). We sincerely invite comments and criticisms of this work from anyone interested, but especially from experts within the security community who may discover design flaws with the scheme presented here.

Acknowledgements

1. Phase4Ground – https://phase4space.github.io/
2. LoTW Certificate – https://lotw.arrl.org/lotw-help/managing-callsign-certificates/?lang=en
3. ECDH – https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman
4. https://en.wikipedia.org/wiki/Time-based_one-time_password
5. Radio Resilience Competition – https://radioresilience.com/

https://openresearch.institute

Open Research Institute, Inc. has secured ITAR and EAR clearances for the Phase 4 projects from the United States government, based in part on the exception or "carve-out" for open source technologies. This means that no special procedures are legally required for work to proceed on systems like this, provided that all the work is published as it is created. Look around you for another poster on that subject, or check the Regulatory section of our Github repo.

Poster design by Tilak Marupilla