

EVIDENCE DOSSIER

Aviation VHF Voice Authentication — Citation Spine

A structured reference for journalists, researchers, and staff

July 2026 · Companion to <https://haijacked.com/evidence> · Policy brief: <https://haijacked.com/brief.pdf>

This dossier restates every operative factual claim used in the HAIJACKED campaign materials, with attribution. It is intended to be copied from accurately. Prefer this document or the live evidence page over secondary paraphrase.

A. The Vulnerability

Aviation VHF voice communication operates on unencrypted analog channels, 118.0–136.975 MHz. There is no cryptographic authentication, no digital signature, and no challenge-response mechanism — stated explicitly in Vu & Wei (2026), § III threat model. Pilots comply based on four cues: the voice sounds like the controller; it arrives on the expected frequency; it uses correct phraseology; and it is contextually plausible. Phraseology and ATM procedure are governed by ICAO Doc 4444; that document does not assert the absence of cryptography. The openness is deliberate and operationally valuable — pilots need to hear other traffic — which is why encryption has consistently been rejected for this layer.

B. Public Demonstration (2025)

Event: DEF CON 33, Sunday, August 10, 2025.

Presenter: Andrew “Helicopters of DC” Logan — describe as “audio engineer and aviation-transparency researcher” (not merely “a researcher”).

Title: “Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings.”

Venue: Main DEF CON speaker track — **not** the Aerospace Village.

Content: Demonstration of using a cloned controller voice to instruct an aircraft to cross an active runway in front of landing traffic.

Coverage: *Aviation International News*, August 22, 2025, headline: “DEF CON Talk Warns of ATC Voice Cloning ‘Nightmare.’”

Links: AIN — <https://www.ainonline.com/aviation-news/2025-08-22/def-con-talk-warns-atc-voice-cloning-nightmare> ; Talk recording — <https://www.youtube.com/watch?v=JKwxsGYcZq4>

C. Peer-Reviewed Research (2026)

Authors: Dao Vu and Peng Wei, George Washington University.

Title: “Generating Realistic Air Traffic Control Voice Communication using AI-based Text-to-Speech Models.”

Venue: IEEE ICNS 2026 — 26th Integrated Communications, Navigation and Surveillance Conference, Herndon, Virginia, April 14–16, 2026.

Form: Always “peer-reviewed conference paper.” Never imply a journal.

Evaluation: 1,000 authentic controller utterances from the ATCOSIM corpus (§ V-A).

Results (§ V-B, Table I): Word error rate 3.9% (median 0%); critical-token F1 = 0.958; speaker-embedding cosine similarity 0.726. Same-speaker verification typically reaches ≥ 0.8 for the same utterance — so 0.726 across different utterances is the striking figure.

Threat model (§ III, verbatim): “an adversary capable of generating synthetic ATC-style audio conditioned on publicly available recordings of controller speech... exploiting the absence of cryptographic authentication and encryption in legacy VHF voice communication architectures.”

Limitation named by authors (§ VI): Prosody/cadence weakest-reproduced; evaluation “without explicit VHF channel modeling, radio compression artifacts, or environmental noise injection.”

PDF:

<https://bpb-us-w2.wpmucdn.com/web.seas.gwu.edu/dist/9/15/files/2026/04/Dao-DeepFakeATC-Comms-ICNS26.pdf>

D. The Funding Gap

\$12.5 billion appropriated for ATC modernization in the reconciliation bill signed July 4, 2025; approximately \$20 billion additional requested; total: more than \$32 billion. Target completion: end of 2028. Directed at: replacement of up to 612 legacy radar systems by June 2028; migration of legacy copper telecommunications to fiber, satellite, and wireless (approximately 40% complete); facility replacement. **None of it authenticates the voice carried on the frequency.**

E. Staffing

FAA entered 2026 approximately 3,544 certified controllers below its own staffing target. According to NATCA, more than 41% of certified controllers work 10-hour days, six days per week (NATCA figure). On May 15, 2026, FAA revised its staffing target downward from 14,633 to 12,563.

F. Historical Precedent

Documented incidents (each with date): USAir diverted on approach to Reagan National by unknown voice (April 1999); transmitter stolen from Edinburgh Airport used for false commands (December 1999); ham radio operator at Manchester (1999); East Midlands controller transmitted “Respond to my voice only” (July 2000). Drawn from a single contemporaneous wire story (ABC News, August 29, 2000), which itself cites the Sunday Times for East Midlands; SKYbrary summarizes the same attack class.

Important context: These incidents are ~26 years old; three of four are British. They establish that the attack class is old. They establish nothing about the present. The read-back / incorrect-phraseology defense that made them low-severity then is precisely what synthetic speech undermines now.

As far back as 2000, the FAA acknowledged that unauthorized people periodically use controller frequencies to issue false instructions, including ‘ghost transmissions’ at JFK. Reporting at the time indicated that no capability existed to block or filter such broadcasts. We are not aware of any deployed since. A widely repeated line that “the FAA says no technology exists to block these broadcasts” originates as a reporter’s paraphrase in that 2000 article, not as a current agency statement. It is twenty-six years old and should not be read as the FAA’s present position.

G. Legal

Criminal: 49 U.S.C. § 46308 (up to 5 years); 18 U.S.C. § 32 including § 32(a)(8) (up to 20 years); 47 U.S.C. § 333. Synthetic-media statutes (TAKE IT DOWN; AI Fraud Accountability Act of 2026; NO FAKES Act of 2026) are directed elsewhere. Gap formulation: no federal synthetic-media statute reaches impersonation of a safety-critical operator; general aviation-interference statutes predate synthetic voice and punish afterward without requiring detection capability.

H. Unverified

- DOT OIG finding (reported April 2026) that FAA lacked baseline security controls on ~10% of “high-impact” ATC systems — not confirmed here from the OIG report itself.
- Reported January 2021 arrest in Berlin for repeated ATC impersonation — not confirmed here.

I. Correct Names and Descriptions (Copy Desk)

NAME / TERM	USE THIS DESCRIPTION
-------------	----------------------

Andrew “Helicopters of DC” Logan	Audio engineer and aviation-transparency researcher; DEF CON 33 main track
Dao Vu / Peng Wei	George Washington University
IEEE ICNS 2026	26th Integrated Communications, Navigation and Surveillance Conference; peer-reviewed conference paper
NATCA	National Air Traffic Controllers Association
ATCOSIM	Corpus of authentic controller utterances
Ernie Ortiz	Retired air traffic controller; technical adviser
Sunny Paul Smith	Author

J. What We Do Not Claim

We do not claim this attack has been carried out. We do not claim any specific airport is vulnerable. We do not claim to know what capabilities the FAA may have deployed and not disclosed. We do not claim the novel’s scenario is a forecast. We claim that this layer is unauthenticated, that it has been publicly demonstrated, and that the current modernization program does not appear to address it.

Press contact and interview availability: <https://haijacked.com/press>. Corrections: <https://haijacked.com/humans.txt>. No ATC audio — real or synthetic — is hosted or demonstrated on haijacked.com.