5 January 2012

Report from Chairman,
IGC GNSS Flight Recorder Approval Committee (GFAC)
to the IGC 2012 Plenary

Author: Ian Strachan, GFAC Chairman

IGC Plenary agenda para 8.2.4

Appendix 3 to GFAC Chairman's report

Introduction. At their meeting on 8-9 October 2011, the IGC Bureau considered a paper on FR security from the ANDS and GFA Committees (Reference B below) and agreed the proposed changes to the IGC-approval levels for a number of old Flight recorders. These changes are summarised in the paper that follows, are recommended to take place on 31 March 2012, and the full case is at Reference B.

IGC Flight Recorder Security and Recommendations

References: A. Para 5 of main GFAC report
B. ANDS/GFAC security paper - has been made available through the GFAC Chairman's web site:
www.ukiws.demon.co.uk/GFAC and the paper itself is at:
www.ukiws.demon.co.uk/GFAC/documents/igc%20fr%20security%202011-10a.pdf
In due course it will also be available on the IGC web pages but in 2011 there were major problems with the FAI web server. At the time that this report is written, it was not available on the IGC pages.

1. **Background**. Earlier in 2011 GFAC was notified by an NAC that a false IGC file had been submitted to their OLC that continued to pass the IGC electronic Validation check. The file was for a 750km triangle and had been submitted as if it was a real flight. The NAC reported to GFAC that a false file had been submitted and action followed by GFAC and the IGC ANDS committees.

2. **Analysis**. In the false IGC file, code-breaking ("hacking") techniques had been used to create a security record at the end of the file that enabled it to pass the IGC Validation check. Experts in electronic security from ANDS, GFAC and the NAC confirmed that types of IGC-approved FRs approved in the 1990s including those using public/private key systems (such as RSA [1]) with low public key lengths, are now particularly vulnerable to hacking. This would allow completely false IGC files to be produced that would pass the IGC Validation check. Further details on electronic security are in Annex A to Reference B.

3 **Actions by ANDS and GFAC.** After initial notification and analysis of the false file, ANDS and GFAC took the following actions.

3.1 FR Technical Specification. An amendment to the FR Technical Specification was made to increase security in the future. The minimum private key length for future "all flights" approval was increased to 1536 bits, and other security matters were tightened up.

3.2 Vulnerable IGC-approved FRs. Recommendations are to reduce the IGC-approval level of 8 types of FR and to withdraw IGC-approval from 4 types. These all have initial approvals from the 1990s, except for one in which private keys were revealed by the manufacturer who in no longer making FRs.

3.3 FR-approval change procedures. The current procedures for reducing IGC-approval levels are given in Appendix A to Annex B to the Sporting Code (SC3B). However, after seven years of operation the approval-change procedures have never been used (until now), and in the view of the ANDS and GFA Committees the procedures are bureaucratic and cumbersome. Simplification is recommended, particularly where security and hacking issues are involved that could lead to false flights being validated.

[1] RSA is a commonly-used electronic security system using the Public/Private key principle. For more details, see the Glossary at the beginning of the IGC FR Specification.

4 **OO Supervision**. For flights to be validated to IGC standards, the time between landing and initial download of the IGC file by the OO should be as short as possible. Furthermore, the OO should personally perform the download rather than allowing the pilot or anyone else to do so. In addition, to preserve the independence of the download process, the OO should not use any hardware or software owned by the pilot or anyone else, other than the FR itself. For more detail, see Annex A to Ref B, particularly para A5.1.

4.1 SC3 Changes Proposed. Wording in SC3, SC3C (and SC3A where relevant) should be strengthened in these areas. The SC3 Committee is invited to note and take appropriate action.

5 **Recommendations for Change of IGC-approval Level**.
To put these in perspective, there are currently 50 types of IGC-approved Flight Recorders. The complete list is available through the GFAC Chairman's web site:
www.ukiws.demon.co.uk/GFAC , the exact reference being as follows:
www.ukiws.demon.co.uk/GFAC/igc_approved_frs.htm
In due course this will also be available through the IGC web pages (in 2011 there were major problems with the FAI web server and updates and new IGC documents were not available for some time).

5.1 Reductions to Diamonds Level. The following FRs have either low private key lengths, or in the Cambridges and Zander GP940, a "symmetrical"security system not based on public/private key:

Cambridge 10, 20, 25
Filser/LXN DX50
Filser/LXN LX20, later models with RSA192
Filser/LXN LX21
Filser/LXN LX5000 IGC
LXN Colibri 1
SDI/LXN Posigraph
Zander GP940

5.2 Withdrawals of IGC-approval. The following FRs are not considered to be secure enough to be approved as IGC FRs. If an NAC considers it appropriate, one or more could be listed as IGC Position Recorders for Silver and Gold badge flights.

All are out of production and no longer have manufacturer support.

EW FR A-D with separate GPS receiver (no significant security)
Filser/LXN LX20, batch 1 without RSA (already cracked in 1997)
Print Technik GR 1000 without RSA (similar to LX20 batch 1, above)
Print Technik GR 1000A with RSA (the company revealed private keys in the Public Domain).

6 **IGC-approval Change Procedures**. It is recommended that SC3B Annex A be shortened to the following:

APPENDIX A
CHANGES OF IGC-APPROVAL LEVEL

A1 Changes of approval level. If GFAC proposes to lower the approval level of a type of IGC-approved recorder, this will be discussed in confidence with the manufacturer and then with the IGC ANDS Committee. As much notice as possible will be given to the manufacturer so that there is the opportunity of offering an upgrade that will retain the existing approval level. The IGC Bureau may also be informed if appropriate.

A1.1 After these discussions, if GFAC still decides to recommend a lowering of the approval level it will then make a detailed recommendation to the IGC Bureau. The Bureau will then assess all of the evidence and make a decision. To aid this process, the Bureau may decide to make a public request for comments (avoiding any confidential or proprietary information).

A1.2 If the decision is to lower the approval level, this will be announced on the IGC web page, to the FAI IGC discussion group (igc-discuss@fai.org) and on the international soaring newsgroup (rec.aviation.soaring) avoiding confidential or proprietary information. The next IGC Plenary meeting will be informed as part of the normal procedure for confirmation of Bureau decisions that were made between Plenaries.

A2 Factors in Lowering Approval Levels. These include the following.

A2.1 False Data. Evidence that flight data from an IGC-approved recorder has been, or can relatively easily be, manipulated or altered. For instance, if it can be shown that the secure areas in an IGC file (Such as data in a B- fix-record line(s)) can be changed and the file continues to pass the IGC electronic Validation check.

A2.2 FR Security. Evidence that the security of the FR itself has been compromised, or could relatively easily be compromised. This includes where security devices in the FR could be by-passed.

A2.3 Dates of Change. In the above cases, the lowering of IGC-approval level will take effect at a date agreed between ANDS/GFAC and the Bureau. Where there is a risk that compromised data could be submitted for flight claims from other recorders of the same type, this could be a date soon after the public announcement of the Bureau decision.

A2.4 Other factors. If the approval level is to be lowered for reasons other than those above, the date of implementation will be decided by the Bureau. This will not normally be less than between 6 and 12 months after the date of the public announcement of the Bureau decision.

A4 Appeal against a lowering of approval level. The manufacturer of the recorder or any entity with a direct interest (which must be shown in the appeal papers) in that type of recorder (the "appellant") may appeal to the IGC Bureau to have the decision reviewed. Pending the result of the appeal, the decision and its implementation timescale will stand.

A4.1 Making an Appeal. Within one calendar month of the public announcement, the appellant must notify the IGC President, and pay an appeal fee of 500 Euros to the IGC account at FAI [2]. The fee is refundable if the appeal is upheld. The full case for the appeal must be received by the IGC President or his nominee within a further calendar month. Communication should be by email and include attachments, pictures and diagrams as appropriate.

A4.2 Appellant's Agreement. In submitting the appeal, the appellant agrees to accept the result, which is at the sole discretion of FAI as the legal entity, its agent IGC, its agents the IGC Bureau, Committee members and advisors. The appellant also agrees not to institute proceedings against the FAI or its agents including any person who was involved on behalf of FAI or IGC.

A4.3 Appeal Evidence. The appeal must include evidence in support so that the Bureau can assess it and consider whether their previous decision should be changed. Where technical evidence is submitted, this will be assessed by technical experts nominated by the Bureau which will include the ANDS and GFA Committees and their technical advisors, and, where necessary, independent experts.

A4.4 Decision on the Appeal. The decision on the appeal is the responsibility of the IGC Bureau, but it may nominate specific members and/or experts to deal with the detail of the appeal and make recommendations to the full Bureau. A decision will normally be made within one calendar month of receiving all of the evidence from the appellant, but if technical detail has to be assessed the timescale may be longer. The decision will be sent to the appellant before any public announcement is made.

---

[2] References for the FAI account are available from the FAI office and the Chairmen of the IGC ANDS and GFA Committees