ANDS/GFAC paper on security of IGC-approved Flight Recorders

Part 1 - The Bureau Meeting of the FAI Gliding Commission 8-9 October 2011

Extract from the Bureau minutes: "13. ANDS/GFAC paper on security of IGC-approved Flight Recorders. The Bureau agreed to the proposed changes related to old Flight recorders. GFAC to publish the proposed changes at the IGC web."

The paper referred to above follows, see para 4 for the changes that were recommended. In accordance with line 3 and 4 of para 4, the GFAC Chairman's report for the agenda of the annual IGC Plenary meeting on 2-3 March 2012 recommends that the changes take place on 31 March 2012.

Although the paper was sent for publication on the IGC web pages, due to difficulties after the crash of the FAI web system earlier in 2011, availability on FAI/IGC web pages was considerably delayed.

However, for some time it has been available through the GFAC Chairman's web site:
www.ukiws.demon.co.uk/GFAC . For the paper itself see:
www.ukiws.demon.co.uk/GFAC/documents/igc%20fr%20security%202011-10e.pdf

Part 2 - The ANDS/GFAC Paper

To: IGC Bureau
Copy: Chairmen IGC Annex A and Sporting Code Committees

From: Chairman GFA Committee, on behalf of ANDS and GFAC
Date: 19 July 2011

IGC-approved Flight Recorders - Security

Summary.

A significant security breach occurred earlier in 2011, in which an IGC file was submitted to a National OLC that passed the IGC electronic Validation check, but critical data in the file was shown to be false.

Actions followed by the ANDS and GFA Committees. These included an amendment to the Flight Recorder (FR) Specification to increase future security. At the same time, a security survey was started for existing IGC-approved FRs and their IGC files.

The survey has so far showed that several types of early IGC-approved FRs are particularly vulnerable to the breaking of their electronic security codes ("hacking"). If hacked, false IGC files from these FRs can be produced that will continue to pass the IGC electronic Validation check.

Recommendations to the IGC Bureau include withdrawing IGC-approval from some early FRs, lowering the IGC-approval level of some others, streamlining and co-ordinating the procedures for Grandfather rights, and tightening up some OO procedures.

The background and justification for these recommendations are given in this paper. Meanwhile the security survey continues and other options for the future are being considered such as web-based Validation.

IGC-approved Flight Recorders - Security

1. **Background**. Earlier in 2011 GFAC was notified by an NAC that a false IGC file had been produced that continued to pass the IGC electronic Validation check [1]. This file was for a 750km triangle and had been submitted to the NAC's own OLC as if it was a real flight. However, the Header record of the file showed the glider as a K-13 and the two named pilots were well-known competition pilots who had not flown a K-13 together, let alone for 750km.

1.1 A copy of the IGC file was sent to the GFAC chairman who forwarded it to the ANDS and GFAC committees and their advisors for analysis. It was confirmed that the file passed the IGC electronic Validation check. The security system used the well-known "Public/Private Key" method where resistance to hacking depends on the length of the Private Key [2] .

2. **Analysis**. The false IGC file contained flight data from a real flight but its Header record had been "doctored" with a false aircraft type and crew. It could be taken as an attempt to show that this method of cheating was feasible. 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 [3]) 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, including those more serious and less detectable than an obvious alteration of the file Header. Further details on electronic security are in Annex A.

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 Specification. Extensive discussion was held on an amendment to the FR Technical Specification to increase security in the future [4]. The minimum private key length for future "all flights" approval was increased to 1536 bits, and other security matters were tightened up.

3.2 Security Review of Existing FRs. At the same time as developing the Specification amendment, FR manufacturers were contacted so that their FR security systems could be confirmed. This was because after GFAC was created in March 1995, manufacturers were reluctant to reveal their security systems and it is only in the last few years that it has been required that exact details had to be given.

3.2.1 The FR Specification. The initial version of the Specification was issued in October 1997, in which it was mandatory to use a Public/Private Key system such as RSA. Private keys of 192 bits

---

[1] Electronic Validation of an IGC file is a part of the free IGC Shell program that was developed by the USA member of GFAC (previously via FR manufacturers' short VALI program files). IGC Validation checks that the file has originated correctly from the appropriate type of IGC-approved FR, that the FR has not been interfered with, and that the file is identical to when first downloaded.

[2] The Flight Recorder (FR) concerned was an early model LX-20 with a private key length of 192 bits, originally IGC-approved in 1998. Under Grandfather Rights procedures, this version of the LX-20 continues to be IGC-approved for "all flights", although the private key size for "all flights" IGC-approval had been increased to 512 bits in May 2001 and to 1536 bits in May 2011.

[3] 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] Initially it was hoped to issue the Specification change at the end of April but the complexities of defining future security systems meant that the issue date was the end of May.

were used in a number of types of FR [5]. Amendments to the Specification increased this to 512 bits in May 2001 and to 1536 in May 2011.

3.2.2 Vulnerable IGC-approved FRs. A table listing the main types of FR in date order of their initial IGC-approval is at Annex B. This includes the recommendations in Para 4 and links them to the security systems used. Our initial recommendations include proposals 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 one for which private keys were revealed by the manufacturer [6] and was a 1990s design operating under Grandfather rights.

3.2.3 Numbers of IGC-approved FR types. On the IGC/GNSS web pages, 50 different types of IGC-approved FR [7] are currently listed. This is more than those listed in Annex B because some of the latter have sub-types with the same security system which are listed separately in the table.

3.2.3 The 2011 Security Review. The security review deliberately covered subjects wider than the circumstances of the security breach earlier in 2011, which was used as the trigger for this, the first such review since GFAC was formed in March 1995. The review is ongoing but there is enough evidence at this time to make the recommendations in para 4. Other recommendations will follow.

3.2.4 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). They were introduced by the Bureau in 2004 after the current system of three IGC-approval levels was set up. Originally there had only been one approval level, but by 2004 a wide range of FR characteristics and security systems had been produced. A single approval level was therefore considered too inflexible and could lead to recorders suitable for flights below the world record level being denied any form of approval, even for lower-level badge flights. 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.

3.2.5 FR Grandfather Rights. The current rules and procedures for "Grandfather Rights" allow old types of FR to retain their original IGC-approval level "even though the provisions of the IGC Specification or Sporting Code have changed" [8]. In the future, IGC-approvals could be time-limited rather than open-ended. This would depend on the security system used in a particular type of FR and the state of computing (and hacking) at a given future time. In general, a period of between 5 or 10 years (to be decided) could be followed by a review of the particular FR type in terms of security and other characteristics. The approval would then be re-issued unchanged, or changes would be required before re-issue, or the process for reduction of approval level would apply, or for withdrawal of approval. There will always be an anomaly in requiring higher levels of security for new equipment while equipment with lower security can be used for the same performance; someone who wishes to cheat will focus on a low-security FR. The balance between the ideal situation where

---

[5] In 1997 the security of an early non-RSA LX20 FR was cracked and it was because of this that RSA or equivalent became mandatory.

[6] This FR has a NiCad sustainer battery that discharges quicker than sustainer batteries used in other FRs and computers. When the battery is discharged, security is lost and needs to be re-set. The company gave out Private Keys so that owners could carry out their own re-sets, rather than the usual procedure of return to the manufacturer or an agent authorised to carry out a security re-set.

[7] www.ukiws.demon.co.uk/GFAC/igc_approved_frs.htm

[8] See Annex B to the Sporting Code, para 1.1.4.5

security is the same, at the same time allowing for owners of older equipment in a fair way, is a political rather than a technical judgement.

3.2.5.1 The Current Cycle. The above would avoid repeating the current cycle of (1) increasing the level of security in the Specification, (2) having a security breach in an approved FR type, which will probably be a Grandfathered one with less security than in the current Specification, then (3) having to fix the situation. As we are now doing.

3.3 Applications for IGC-approval. After the Specification amendment and the start of the security survey of existing FRs, in June 2011 the application forms and data that is requested of applicants for IGC-approval were updated. This "cleared the decks" for this paper to be produced for the IGC Bureau.

4. **Recommendations to the IGC Bureau**. Recommendations involving changes to FR approval levels under paras 4.2 and 4.3 are based on the table at Annex B that lists the security systems used by types of IGC-approved FRs in date order of initial approval. The date of changes of FR approval level is to be agreed by the IGC Bureau, but should not be later than shortly after the date of the 2012 IGC Plenary meeting, to which in any event a case and proposals should be put.

4.1 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. [9] . More detail is given in Annex A, particularly para A5.1.

4.1.1. 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.

4.2 Recommended from All Flights to Diamonds Level. The following types of FR are not considered to be secure enough to be used for world records, and in view of the vulnerability of low private key lengths should now be set at Diamonds level:

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

4.3 Recommended reductions from All Badge/Diplomas to Diamonds.

Cambridge 10, 20, 25 - In security terms these are similar to the Zander GP940 (see 4.2 above), that is, having a non-RSA security system but with a double key.

4.4 Recommended withdrawals of IGC-approval. The following types of FRs are no longer considered to be secure enough to be approved as IGC FRs. They could be listed by NACs 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)

---

[9] See www.ukiws.demon.co.uk/GFAC/downloads.htm for the latest versions of the IGC shell program and DLL files for different types of FRs

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).

4.5 Other FRs. Since 2001, 512 bit systems have been mandatory for "all flights" approval and the majority of IGC-approved FRs in service today use 512 bits, maybe between 80 and 90% of current FRs. However, para A4.2 indicates that, obtaining the Private Key for a 512 bit system would take hours to days on a moderate size cluster of computers, several weeks to months on a home computer, and 512 bit FRs are therefore vulnerable now to a determined hacker with access to a computer cluster. This should be addressed in the future by an upgrade programme to higher key lengths, also by ANDS and GFAC looking at other methods of security such as web-based systems in which the correctness of the validation software could be more guaranteed than when carried out in the field. Work on this continues and will be reported later.

4.6 Procedures for reductions in IGC-approval levels. The procedures in Appendix A to SC3B should be reviewed with a view to making them shorter and simpler (para 3.2.4 refers)

4.7 Grandfather rights - review. It is recommended that the rules and procedures for Grandfather Rights be reviewed (para 3.2.5 refers), and coordinated with the review of procedures for reductions in IGC-approval levels (para 4.6). The advice of the Bureau is requested on how the procedures for Grandfather rights should be linked to a more streamlined process for reduction of approval levels, particularly where security is concerned.

5 **Conclusion**. After a security breach earlier in 2011 involving a false IGC file that continued to pass the IGC Validation check, the opportunity was taken to start an in-depth review of the security of FRs and their IGC files. This review continues. This is the first such security review since GFAC was formed in March 1995 and is wider than the circumstances of the security breach that led to the review. Some action has already been taken such as an amendment to the FR Specification, and further action is recommended (para 4 above).

This paper covers what ANDS and GFAC have already done, gives the background to electronic security of IGC-approved FRs and their IGC files, and makes interim recommendations to reduce the possibility of malpractice and cheating in the future. This particularly applies to several types of FRs that have security systems well below the current standard. Meanwhile it is recommended that SC3 procedures for OOs are tightened up and that procedures for Grandfather rights and reduction of FR levels are coordinated and streamlined.

Ian Strachan
GFAC Chairman
for the ANDS and GFA Committees

Annexes:

A. Electronic Security - Details
B. Table of IGC-approved FRs in date order with their security systems, and recommendations

---

Annex A - **Electronic Security - Details**

A1. **General**. Public/private key digital signatures are used to validate flight data files produced by FRs that were IGC-approved since the initial version of the FR Specification was published in October 1997. Each individual FR has unique numeric public and *private* keys. For the RSA and DSA algorithms used in most FRs, these keys are functions of a pair of very large prime numbers. The FR calculates a message digest (hash code) for each IGC file, then encrypts it using the *private key*, producing a digital signature unique to the file contents.

A1.1 IGC file Validation The contents of an IGC file are validated by decrypting the digital signature using the corresponding public key, and verifying that the message digest matches the contents of the file. This process checks the security record that is at the end of each IGC file [10] and detects a change of one character in the flight data from that which was originally downloaded. The validation code for a particular FR type includes a database of public keys for the individual FR units of that type, and this is embedded in the FR manufacturer's IGC-XXX.DLL file that works with the IGC Shell program and is available on the IGC FR web pages. As long as the *private key* for a given FR remains secret, a third party cannot alter or create the contents of an IGC file that will continue to pass the IGC electronic Validation check.

A2. **Finding Private Keys**. Due to the mathematical relationships involved, using modern computing resources and the motivation to find a *private key* (loosely, deliberate "hacking") it can eventually be found from the public key after extensive computing. Security is preserved by the size of the keys, and it can therefore be seen that the bit size of the *private key* is critical to resisting hacking.

A2.1 *Private Key* lengths. If the *Private Key* length is small, the computing resources and time required are within reach of a sufficiently motivated individual or group. However, if the numbers are too large, the limited computing resources available in the FR itself will result in a long delay while calculating the digital signature at the end of the flight, delaying the availability of the IGC file. Setting an appropriate key length is a balance between maintaining the integrity of the overall system for some years, while making it possible for the FR manufacturers to produce devices with an acceptable cost and performance. However, as a result of continuing advances in computing technology, FR units in the field with shorter key lengths will eventually become insecure to determined hackers.

A3. **Hacking methods**. The mathematics of this process are well understood, and software is freely available on the internet which can determine the prime factors needed to calculate private keys. For FRs, the necessary information is present in the validation software freely available on the IGC FR web pages. Once the private key for a given FR has been found, altering or creating an IGC file which will pass validation can take a matter of seconds using fairly simple software.

A3.1 IGC FRs. As pointed out in 2.1, it is critical to make sure that the key length used for IGC-approved FRs is appropriate to the computing resources that might be available to an attacker, and it must be understood that FRs with shorter key lengths are vulnerable to these attacks.

A3.1.1 False IGC Files. Using the above techniques, seemingly valid IGC files can be created or altered without any need to tamper with the FR itself.

A4. **Security of current IGC-approved FRs**. With a few exceptions, existing approved FRs use either

[10] The "G record" at the end of each IGC file. See para A3.6 of the FR Specification

the RSA or DSA algorithms, with key lengths of 192, 512, and 1024 bits, depending on the type of FR.

A4.1 Private Key 192 bits. Using the techniques already described, a *private key* length of 192 bits can be found in a few minutes using a typical home computer.

A4.2 Private Key 512 bits. For 512 bits, it would take several weeks to months using a home computer, but only hours to days of computation on a moderate size computational cluster of the sort available at many universities, engineering firms, and financial institutions. Therefore, a determined hacker with access to a computer cluster could find a 512 bit *private key* now. Further, it is now not particularly expensive for a hacker to buy a computer with multiple units, so that what is essentially a high-end computational cluster is available at the hacker's desktop. In the future, as home PCs become more capable, it may not be long before the same can be done on a basic home computer given the time, motivation and hacking skills. In time, the same will apply to systems with a higher bit count.

A4.3 Private Key 1024 bits. Attacking a key length of 1024 bits is now just feasible on a mid to large size computational cluster, but the calculations would take several months. The problem, of course, is that as faster computers and more sophisticated software become available, even a 1024 bit key will be vulnerable to a high-end home computer setup within as little 5 years.

A4.4 Private Key 1536 bits. As a result of the above, GFAC has already increased the minimum key size for future "all flights" IGC-approvals to 1536 bits. This should provide protection against attacks by individuals (but not by large organizations) for 10 to 15 years.

A4.5 The Future. For future systems that are an extension of the above, we may need to consider 2048 bits. This is considered to be the minimum acceptable length for current low security financial transactions needing several months of protection against individuals or small organizations. Such a key length should be possible maintaining acceptable FR download performance with current 16 and 32 bit microcontrollers used by modern FR designs.

A4.5.1 Other systems. ANDS and GFAC are looking at systems other than the traditional ones described in this paper. These are still being developed, and include systems that might allow IGC files to be Validated through specialised IGC/GNSS web pages ("web-based security") that contain the appropriate checking programs that would be completely independent of pilots, OOs, NACs or any other body .

A5. **Insecure FRs**. The LX-20 for which the false IGC file was produced earlier in 2011 had a *private key* of 192 bits. Therefore, FRs with such key lengths should be considered as insecure, and systems with larger bit counts are now vulnerable to attack by a determined hacker. See A4.2 for 512 bit systems (specified in 2001). Having found a key, it is not difficult to write a small software program to automate the process of calculating the *private key* for specific FR types with low key lengths. In the worst case, this could be distributed to other pilots, *who would need to know little more than how to run a program*. Another program could be developed to alter or fabricate flights.

A5.1 Security and the OO. Any IGC file produced by non-RSA and RSA/192 systems has the potential to be altered after flight, or to have been originally produced by another FR, or be a complete fabrication. Systems with higher bit counts are also vulnerable to determined attack (for instance, see A4.2 above for 512 bits and A4.3 for 1024).

This leaves the OO as the vital remaining line of defence.

If an OO verifies that the physical sealing of the FR is intact, downloads using equipment independent of the pilot, and maintains possession of the IGC file until it securely transferred to the Authority that is to Validate the flight performance (the NAC, competition organisation etc), we can be almost certain that the IGC file used for Validation will be the correct one for the flight. See also 5.2.2.

A5.2 Pilot-owned Equipment. Additional vulnerability is where equipment is used that is owned by the pilot or someone associated with the pilot, who wishes to break the security of the system. If an attacker either supplies the computer used to perform the download from the FR, or otherwise succeeds in introducing additional software into the computer which is to be used, it is not difficult to alter the IGC file at some point after the actual download takes place, without the OO being aware that this has taken place. This software could mimic the behaviour of software such as the IGC shell program, and be installed so that it runs in the background with no visible window.

A5.2.1 Portable Storage Media. Unlike floppy disks, USB memory devices and SD cards are not simply passive storage media. Code can be run directly on the storage device, and Microsoft Windows enables programs to run automatically when the device is inserted in a USB port. A hacker could make such a program to mimic a correct download but produce a false IGC file.

A5.2.2 Downloading and Processing to use Controlled Sources. In order to secure the chain of evidence from a potentially insecure FR, OO rules and procedures must ensure three things:

The OO must not use any computer, software, or storage media, which has been supplied by or is accessible to the pilot or associates of the pilot, and,

The OO must personally perform the download, and,

The OO must take possession of the downloaded IGC file until it has been transferred to the authority that is to validate the flight performance. The OO should retain a copy of the file in case there are any queries.

Otherwise, it is not possible to guarantee the integrity of any flight data files produced by any of the FRs that have inadequate key lengths.

A5.3 FRs and Position Recorders. FR types that are particularly vulnerable should have their IGC-approval withdrawn, and recommendations are made the main paper (para 4.4). These types of FR should be considered by NACs for approval as IGC position recorders (PRs) under SC3 procedures. In the opinion of ANDS and GFAC, the rules under which Position Recorders may be approved for Silver and Gold flights, give no significant electronic security.

	Annex B to ANDS/GFAC paper to IGC Bureau - GNSS FR IGC-approvals in date order						Updated 23-10-2011
s/n	**First Appro Date**	**FR Maker**	**FR Model**	**Current Appro Level**	**Security system & Private Key length**	**Changes**	**Remarks**
1	16-Jan-96	Cambridge	10, 20, 25	Badges (all)	non-RSA with double key	Reduce to Diamonds	
2	31-May-96	Peschges	VP8	Badges (all)	RSA 512		Company no longer making FRs
3	10-Nov-96	Zander	GP940	All Flights	non-RSA with second algorithm	Reduce to Diamonds	
4	12-Aug-96	Filser (now LXN)	LX20 batch 1	Badges (all)	non-RSA, already hacked	Withdraw approval	
5	20-Mar-97	Print Technik	GR1000	Badges (all)	non-RSA	Withdraw approval	Company no longer making FRs
7	25-Mar-97	Filser (now LXN)	LX20 with RSA	All Flights	RSA 192	Reduce to Diamonds	
6	19-Apr-97	EWFR	A-D (separate GPS)	Diamonds	None	Withdraw approval	Separate GPS receivers, no viable security
7	03-Apr-98	Garrecht	Volkslogger VL1	All Flights	DSA 512		
8	24-Apr-98	Filser (now LXN)	LX21	All Flights	RSA 192	Reduce to Diamonds	
9	19-May-98	Filser (now LXN)	DX50	All Flights	RSA 192	Reduce to Diamonds	
10	30-Jun-98	Filser (now LXN)	LX5000IGC	All Flights	RSA 192	Reduce to Diamonds	
11	31-Aug-98	LXN	Colibri 1	All Flights	RSA 192	Reduce to Diamonds	
12	08-Mar-99	SDI/LXN	PosiGraph 1.0	All Flights	RSA 192	Reduce to Diamonds	
13	30-Oct-01	Cambridge	302	All Flights	RSA 512		
14	30-Oct-01	Zander/SDI	GP941	All Flights	RSA 512		
15	31-Oct-02	Scheffel	Themi	Badges (all)	RSA 512		
16	14-Mar-03	LXN	LX7000	All Flights	RSA 512		
17	28-Mar-04	Print Technik	GR1000A with RSA	All Flights	RSA but keys revealed	Withdraw approval	Private keys released in the Public Domain
18	20-Jun-05	LXN	Colibri 4 series	All Flights	RSA 512		
19	08-Aug-05	NTE	Easy Matchbox	All Flights	RSA 512		
20	30-May-06	Aircotec	XC Profi (Gliders)	All Flights	RSA 512		
21	10-Jun-06	EW	microRecorder	All Flights	RSA 512		
22	10-Jan-07	NTE	Easy	All Flights	RSA 512		
23	25-Apr-08	LXN	LX8000	All Flights	RSA 1024		
24	14-Jun-08	EDIATec	ECW100F (Flarm firmware)	Diamonds	Non RSA, boot check system		
25	07-Jun-08	IMI	Erixx V1.0	All Flights	RSA512/SHA256		in 2011: RSA1024/SHA256
26	31-Aug-08	LXN	Red Box Flarm-IGC	Diamonds	Non RSA, boot check system		
27	31-Aug-08	LXN	Mini Box Flarm-IGC	Diamonds	Non RSA, boot check system		
28	10-Mar-08	Flarm	Flarm-IGC V1.0	Diamonds	Non RSA, boot check system		
29	12-Apr-08	DSX	7100 T-Advisor & 8000 Tracer	All Flights	RSA 512		
30	14-Feb-09	Triadis	Altair 1	All Flights	ECC 160 (= RSA1024)		
31	25-May-09	ClearNav Insts	ClearNav-IGC	All Flights	RSA 512		
32	14-Jun-10	LXNAV	LX9000	All Flights	RSA 1024		
33	31-Aug-10	LXNAV	Nano	All Flights	RSA 1024		
34	14-Mar-11	LXNAV	LX8080F	All Flights	RSA 1024		