AUTHENTICATION IN THE TELECOMMAND LINK TO IMPROVE SECURITY

Calum B. Smith (*ESA Retd*), Agustín Fernández León

European Space Agency
ESTEC Keplerlaan 1, P.O.Box 299
2200 AG Noordwijk ZH, The Netherlands
Email: C.B.Smith@Inter.NL.net, agustin.fernandez-leon@esa.int

ABSTRACT

Currently many spacecraft are susceptible to damage or destruction by malicious telecommands inserted into open, unprotected links. This paper explains how this may be prevented if a telecommand decoder built to the ESA specification [2] incorporating the ESA Authentication Algorithm is used on board in conjunction with the complementary ground equipment. The paper also discusses the implications of the use of full encryption as an alternative or in addition to authentication with particular reference to the non-military missions of the scientific and commercial spacecraft with which ESA is concerned.

TC LINK SECURITY: A BROAD SUBJECT

End to end security of the TC link involves several different communication layers and disciplines. Threats to which it is susceptible range from accidental ones such as system malfunctions, operational errors or environmental noise, to intentional attacks. Attacks could be targeted at (a) breaking data confidentiality (passive traffic analysis), (b) denial of legitimate service through disruption of the link (e.g. RF interference) or (c) attempting to insert illicit Telecommands or modify or replay intercepted legitimate ones (impersonation). Vital though all such issues may be, the field is too wide to be covered by one short paper. Consequently we shall focus on the type (c) impersonation attack that the ESA Authentication Algorithm is specifically designed to counteract.

IMPERSONATION ATTACK: A PARTICULARLY SERIOUS THREAT TO A COMMAND LINK

Rules for the generation of a CCSDS/ESA Telecommand Frame are necessarily in the public domain [1][2]. Similarly, details of commercial spacecraft platform design and components [3] are widely known. Also, low cost CCSDS compatible ground equipment is now available, although even without it anybody with a PC, simple RF equipment and a modicum of knowledge of on board systems could generate and send destructive CCSDS compliant TC frames to a near-earth satellite. Thus the consequences of a successful attack could be much worse than just losing the confidentiality of the TC traffic. It is obviously only a matter of time before persons of similar mentality to those who create computer viruses turn their attention to this form of "space terrorism". Examples of impersonation attacks have already been openly reported [7], and, though not as widely available, cases of military satellites attacked by a second illicit up link are reported on the Internet [8]. In effect, any near earth spacecraft is at risk.

ENCRYPTED AUTHENTICATION: THE CONCEPT

Some form of strong protection against CCSDS compliant but illicit (impersonated) TC messages is essential. Putting aside for the moment considerations of confidentiality of the data, an authentication system provides such protection by attaching to each finally deliverable data field a signature that varies in an apparently unpredictable way with the content and sequence of the messages being delivered. This is achieved at the sending end by passing each message through a highly non-linear transformation process involving a large secret key and reduction of the number of bits to the standard signature length. The signature is in effect encrypted, but the issue of encrypting the message is left open. The signature is recomputed on board using the resident copy of the key and message sequence knowledge and if it does not match the one received, the message is blocked from further distribution. If there is any chance of identical message repetition, i.e. message format protocols do not include a guaranteed non- repeating variable such as a sequence count, then this must be implemented by the authentication algorithm itself. By this means, identical deliverable data fields do not produce the same signature. Failure to comply with this would make a successful replay attack possible. The fact that data content and sequence are involved renders detectable any attempt to replay or tamper with the TC frame contents en-route – i.e. it provides end-to-end and temporal protection, including any terrestrial links involved. If the secret key is large, then a well designed algorithm would take a very long time to break [6], even by the most powerful computer. Almost total security may be achieved if new keys are up-linked at much shorter intervals. Resistance to key extraction from the encrypted "change key" messages is very high [6] since good keys look like large random numbers. Consequently the attacker having no "guessable message content" to work from has no *a priori* knowledge of what he is looking for or how close he is to finding it. This renders an attack on key transmission most unlikely to succeed.

THE ESA ENCRYPTED AUTHENTICATION SYSTEM

The CCSDS TC Frame data field (known as the Segment) is the element that is authenticated. The process is fully described in [2] and also in [6]. On the ground, the signature is computed and appended to each Segment as part of an Authentication Tail. The corresponding re-computation and comparison check on board is performed between Frame acceptance (i.e. Data Link Transfer Layer) and presentation to the on board delivery system (i.e. Segmentation Layer). The CCSDS Green Book on general security options [4] for CCSDS compliant missions makes also specific reference to the ESA Authentication algorithm. A short overview of the ESA Authentication system is presented below.

LOGICAL AUTHENTICATION CHANNELS (LAC)

An ESA authenticated Segment has a 72 bit tail comprising a 40 bit signature, a 30 bit LAC count and two bits to identify which of the 3 LAC counters (Main, Auxiliary or Recovery) is being used. The inclusion of the LAC value ensures that identical message contents will not produce identical signatures. It is reported in the Telemetry, so authorized tracking stations can pick up the correct value. The main and auxiliary counters support respectively two authentication channels with a common key but otherwise independent. The third LAC counter is a pointer to a ROM containing one-time keys, a copy of which is also kept securely at the sending end. Each time a one-time key is invoked successfully, the ground and on board LAC 3 counters advance to the next one. These keys are limited in number, only to be used to recover from an otherwise lockout situation e.g. where the on board programmable key value has been corrupted. Typically, only one or two keys would be "burned" in each recovery process. Note that the recovery LAC counter must be utterly stable and non-volatile. Not many technologies meet this requirement. This, and not key storage space, is likely to be the main limitation on the number of one-time keys provided.

THE ESA AUTHENTICATION SIGNATURE GENERATOR.

The first step, the Hashing Function, reduces the data field to a 60 bit long value called the pre-signature. It is performed by a 60 bit linear feedback shift register with programmable but secret feedback taps and so keeps the pre-signature secret. The TC Segment, including LAC value but not Authentication signature, is clocked into this register. Its final state gives the pre-signature. Note also that 3 octets of all zero "virtual fill" are systematically added at the input to this process at both the sending and receiving end since short frames could contain less than the required 60 bits.

The next step involves a process known as a "Hard Knapsack" which is a highly non linear, one-way transformation process. It consists of a matrix multiplication, basically ANDing each bit of the pre-signature with the corresponding bit of each of 60 different 48 bit secret key values, known as weights. This produces 60, 48 bit values that are then summed modulo 2^{48}, resulting in a 48 bit output. Deletion of the 8 LSBs produces the final 40 bit signature and substantially improves the protection provided. Since most of the input data is lost during the transformation process, it is essentially "one-way". That is, although a given input will always result in the same signature, it could just as well have been produced by an astronomical number of alternative inputs. This is a valuable attribute not shared by encryption processes that must be non-ambiguously two-way to decrypt a message.

WHY ESA CHOSE AUTHENTICATION IN PREFERENCE TO ENCRYPTION

By Encryption we mean hiding the content of a message by transposing it from "plain text" to "cipher text". Like Authentication, if the attacker does not have the key, he cannot generate an acceptable message (although unless preventative measures are taken, he can always record and replay an old one!). However, encryption/decryption must be a two way process without loss in either direction to ensure complete plain text recovery. Our main concern is to prevent illicit and destructive commands getting past the Transfer layers and we believe that encryption of all TC traffic by a common process is not the best way to achieve this. In particular, short, easily guessable content commands such as are used for routine spacecraft maneuvering, devastates whatever level of protection encryption may have provided. They give the attacker multiple encrypted and plain text pairs from which, by virtue of the two-way nature of encryption, the key may be extracted with vastly reduced difficulty. Strong enough encryption applied to an "un-guessable" message content could make key extraction almost impossible – as is the case for the "change key" process already described. However, obliging different users on board a commercial or scientific satellite to make their data contents and formats "un-guessable" could be difficult. If one user is careless, everybody suffers

In the commercial or scientific spacecraft environment that is ESA's main concern, the existence, purpose and principal design features of the spacecraft are in the public domain so there is usually no requirement to hide all or even any of the TC traffic. Even if encryption to hide message content were required in addition to intruder access denial, the above considerations led us to the conclusion that we should not attempt to satisfy both requirements by means of a common encryption service in the transfer layers.

Finally, although most often encrypted authentication without message encryption will satisfy non-military requirements, encryption *always* requires some form of authentication in addition to guard against replay attacks. This is essential to a TC link delivering potentially destructive executive commands.

WHEN AND WHERE TO USE ENCRYPTION

Encryption to hide the message content can and should be treated in the appropriate layer as a separate issue from authentication. The argument has been presented for not using encryption in the Transfer layers except perhaps military activities demanding total obscurity at that level. In the commercial / scientific environment under discussion we believe it is more correctly applied independently to each application requiring it. This preserves individual confidentiality for different users of a common TC link and removes the responsibility for encryption key management from operational staff. Also, careless use of encryption by one user, as discussed above, will not compromise the others. More importantly, extracting an encryption key would not help the attacker in the least towards getting a destructive command past the Authentication check.

AUTHENTICATION OVERHEADS : INSTALLATION, OPERATION AND COST IMPACT

As far as the on board segment is concerned, the impact will be insignificant if an ESA Spec. TC decoder with a built-in Authentication Unit, such as in [3], is used. The hardware impact is trivial, and no software is involved since with the exception of the one-time keys, the whole system already resides in the TC decoder chip. There would be some small extra costs involved in managing the creation and installation of the flight ROM with the permanently secret one-time keys. In particular, designs should include the possibility of replacing pre-flight test ROMs with the secret flight component without involving re-qualification. Authentication performance checks would be required, but the effort involved would be trivial, especially if the "Authentication Box" mentioned below is available.

Regarding the ground segment, it might appear that significant extra operational complexity was being added by authentication. However, a well-implemented system would be almost transparent to normal operations and so involve no significant additional operational cost. We have in mind a standard, sealed "authentication box" (fig 1). It would have a small processor board inside plus the standard ESA Authentication generator in ROM. Another ROM would make it mission specific by holding the one-time keys to be used. In use, it would receive unauthenticated TC Segments at its input and compute and add the authentication tail to each one before presenting it externally for forwarding and encapsulation in a TC frame for transmission across the RF link embedded in a Command Link Transmission Unit (CLTU). Like the on-board part, the ground hardware and firmware would be mission independent apart from the pre-mission installed ROM holding the one-time keys. The only other external inputs required are the LAC counter values. These would be visually displayed and would be pre-settable at command session initialization – either manually or automatically via the TM. Key generation and checking processes could be performed by the processor inside the box so that the only other external inputs required would be buttons to initiate internally generated Authentication Control Commands, e.g. for "change programmable key", "select LAC " and "Authentication on/off " etc. Note that nobody requires to know what the key values are, thus eliminating key distribution and management as an avenue of attack. Also, no knowledge or concern with the Authentication process is required by the data source, data sink or intermediate routing system (transparency). Although this assumes authentication will be done at one central point before distribution to tracking stations, multiple authentication boxes could be used on individual tracking stations, but then some safe means of key distribution amongst them would be required.

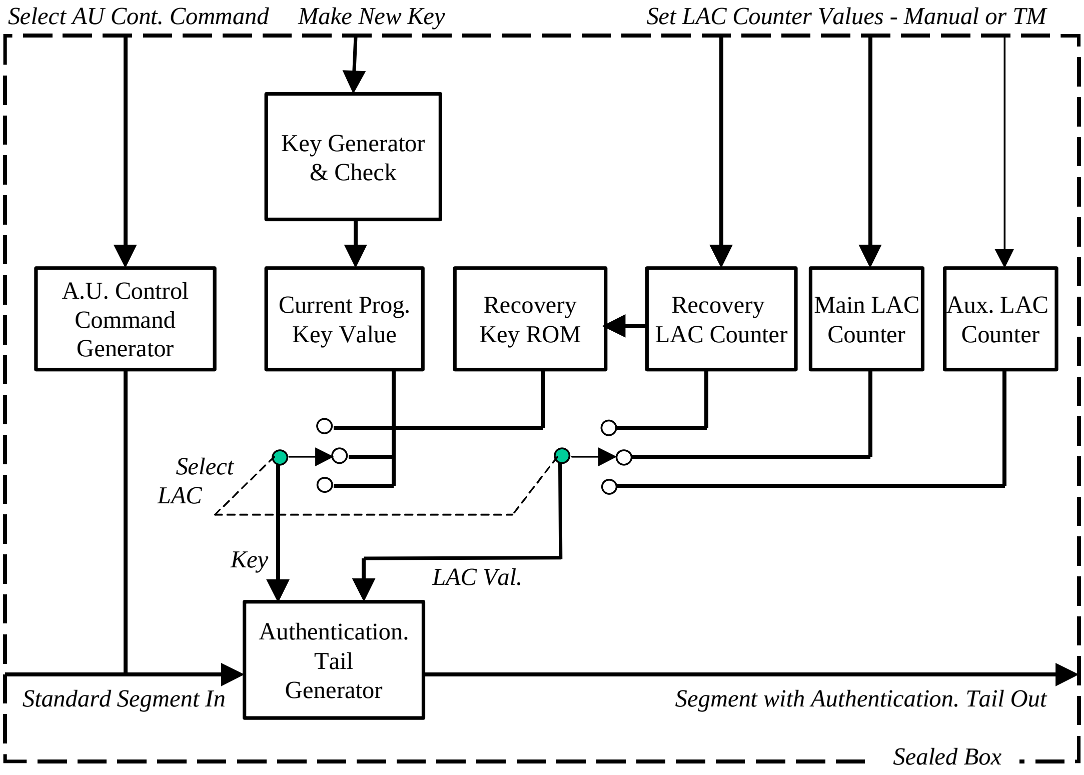

Fig. 1. Proposed Ground Segment Authentication Box.

CONCLUSION

Although improvement is always possible, the current ESA spec. TC Authentication correctly applied is transparent to the messages it protects and provides excellent intruder access denial right across the transfer layers. As applied to commercial and scientific satellites it is more resistant to key extraction and easier to manage than encryption of equivalent complexity without imposing any data format presentation constraints on users. If commercial considerations require message encryption, normally it should be performed in the Application Layer where it would be the responsibility of individual end users to implement and administer it.

REFERENCES

[1] *Packet Telecommand Standard*, ESA PSS-04-107 Issue 2. Paris: ESA, April 1992, ESA.
[2] *Telecommand Decoder Specification*, ESA PSS-04-151 Issue 1. Paris: ESA, September 1993.
[3] *Packet Telecommand Decoder*, PTD MA28140 Data Sheet. DYNEX Semiconductor, 15 June 2000.
[4] *The Application of CCSDS Protocols to Secure Systems*, CCSDS 350.0-G-1, Green Book. Issue. Washington, D.C.: CCSDS, 1.March 1999
[5] *Telecommand Part 1 -- Channel Service*, CCSDS 201.0-B-3, Blue Book. Issue 3. Washington, D.C.: CCSDS, June 2000
http://www.ccsds.org/blue_books.html
[6] *Study for the Improvement of Cryptosystems for Meteosat Image Data and ESATelecommand Data*, Final report ESTEC Contract 7881/88/NL/PP(SC). Paris: BERTIN et Cie, March 1990
[7] MED-TV: A Target of Historic Satellite Sabotage. Lond MED Broadcasting Ltd.: London , March 1995: http://www.ib.be/med/med-tv/pr/jamming.htm
[8] Satellite failure: US suspects sabotage by cyber hackers. May 1998 Indian Express Newspapers (Bombay) Ltd. http://www.expressindia.com/ie/daily/19980525/14550264.html