AUTHENTICATION

in the Telecommand Link to Improve Security

Calum B. Smith, Agustín Fernández León

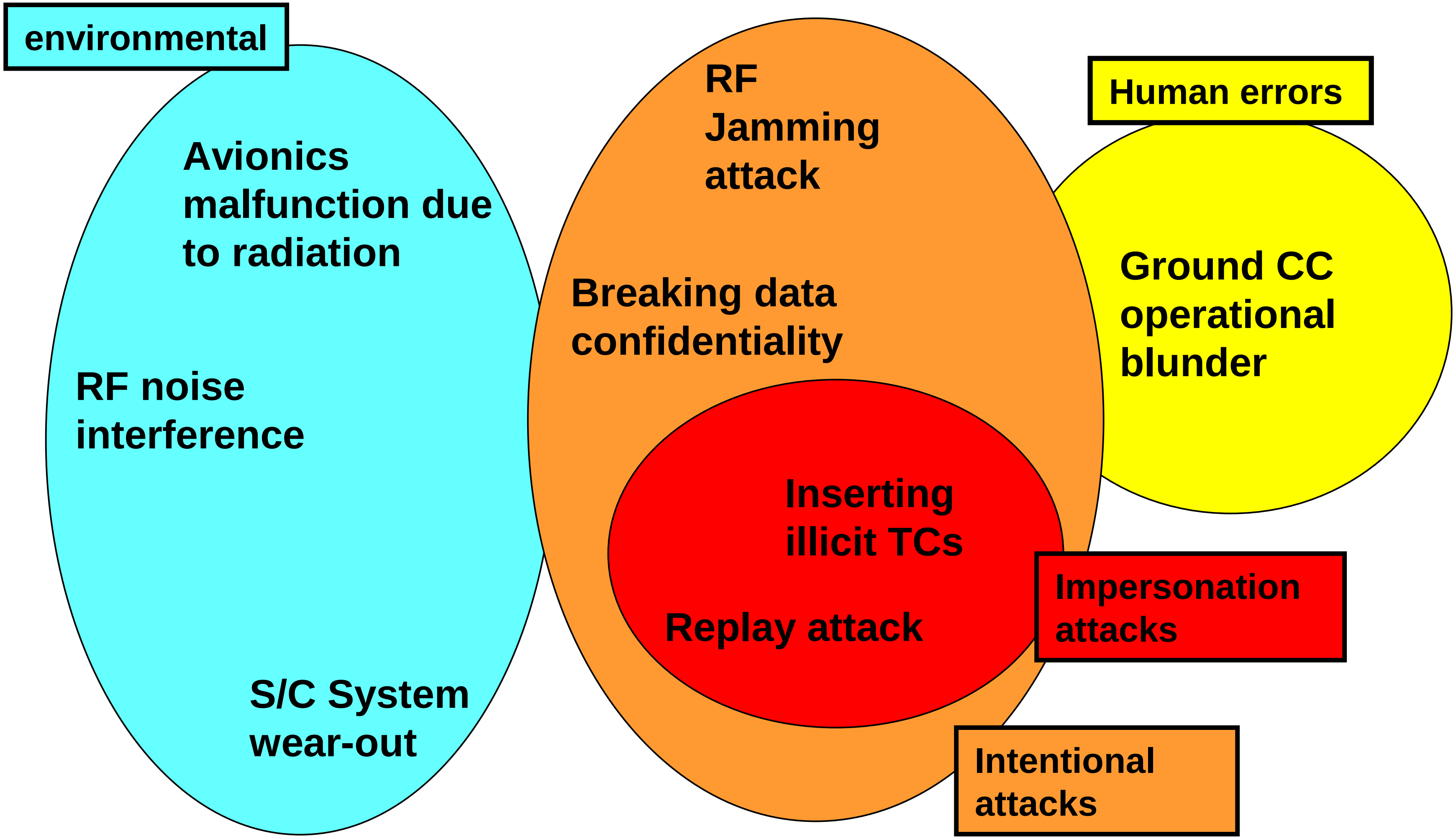
Outline

- THREATS TO THE TC UPLINK
- IMPERSONATION ATTACK
- AUTHENTICATION: THE CONCEPT
- ESA AUTHENTICATION
- ENCRYPTION vs. AUTHENTICATION
- AUTHENTICATION OVERHEADS
- CONCLUSIONS

TC Uplink Security

- End-to-end security: very broad subject
- Many, diverse threats
  - Accidental / Intentional
  - Environmental / Human induced
- Wide range of security measures
  - various disciplines: RF, radiation, cryptology, etc
  - Several Communication Layers and Subsystems involved

A few threat examples ...



IMPERSONATION ATTACKS

Inserting illicit TCs

Replay attack

- Cases already openly reported
- CCSDS/ESA TC formats are public domain
- Ground equipment to send TCs is relatively cheap, easy to assemble and run
- Any near Earth S/C is a potential target

Severe consequences: Satellites can be **hijacked** or **destroyed**.

AUTHENTICATION : the concept

Mechanism to detect and discard illicit TCs

On ground: A binary “signature” is generated and inserted in the TC frame.

On board: The incoming TC’s signature is compared to a signature generated on-board. If signatures match, the TC will be accepted as valid (coming from an *authentic* source) and, otherwise, it will be rejected.

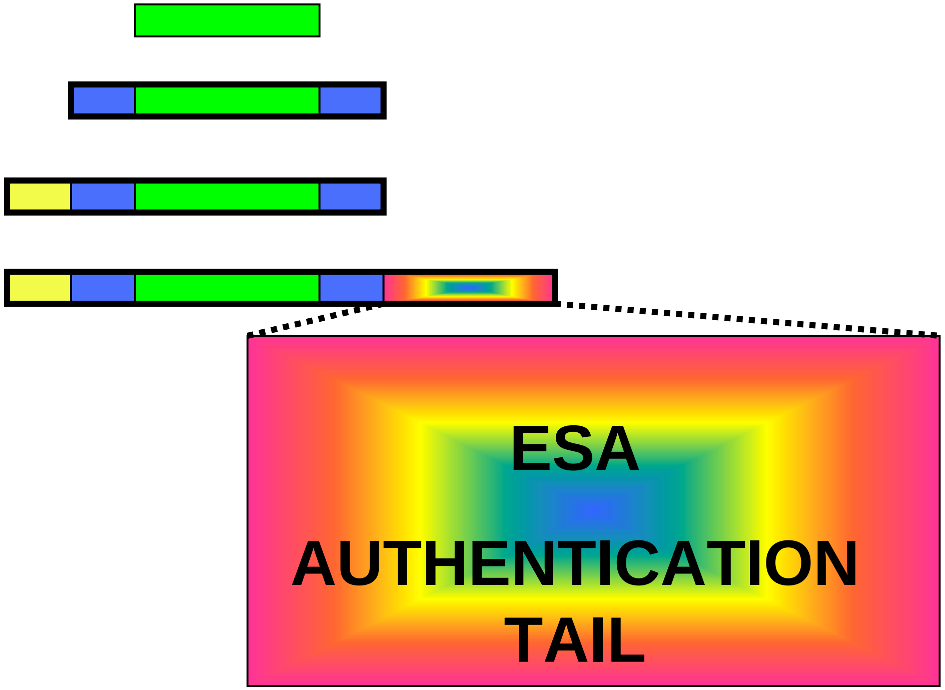
The signature of each TC being sent must be virtually impossible to guess or reproduce by a non authorised party

ESA Authentication

1993 ESA PSS-04-151 “TC Decoder Specification” describes in detail ESA AU

1999 CCSDS 350.0-G-1 “The Application of CCSDS Protocols to Secure Systems”

Application	**data**
Packetisation	**Packet**
Segmentation	**Segment**
Authentication	**Authenticated Segment**

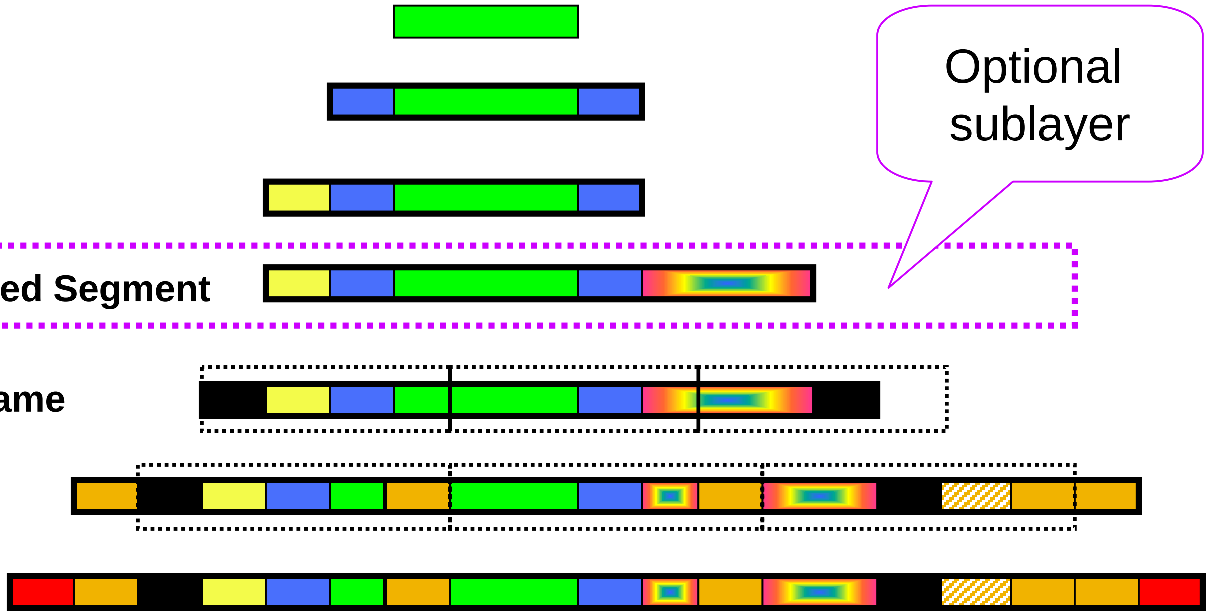


ESA Authentication

1993 ESA PSS-04-151 "TC Decoder Specification" describes in detail ESA AU

1999 CCSDS 350.0-G-1 "The Application of CCSDS Protocols to Secure Systems"

Application	**data**
Packetisation	**Packet**
Segmentation	**Segment**
Authentication	**Authenticated Segment**
Transfer	**Transfer Frame**
Coding	**CLTU**
Physical	**PLOP-1**



ESA Authentication Tail (1): The LAC

LAC (Logical Authentication Channel) = LAC Count + LAC ID

LAC count:

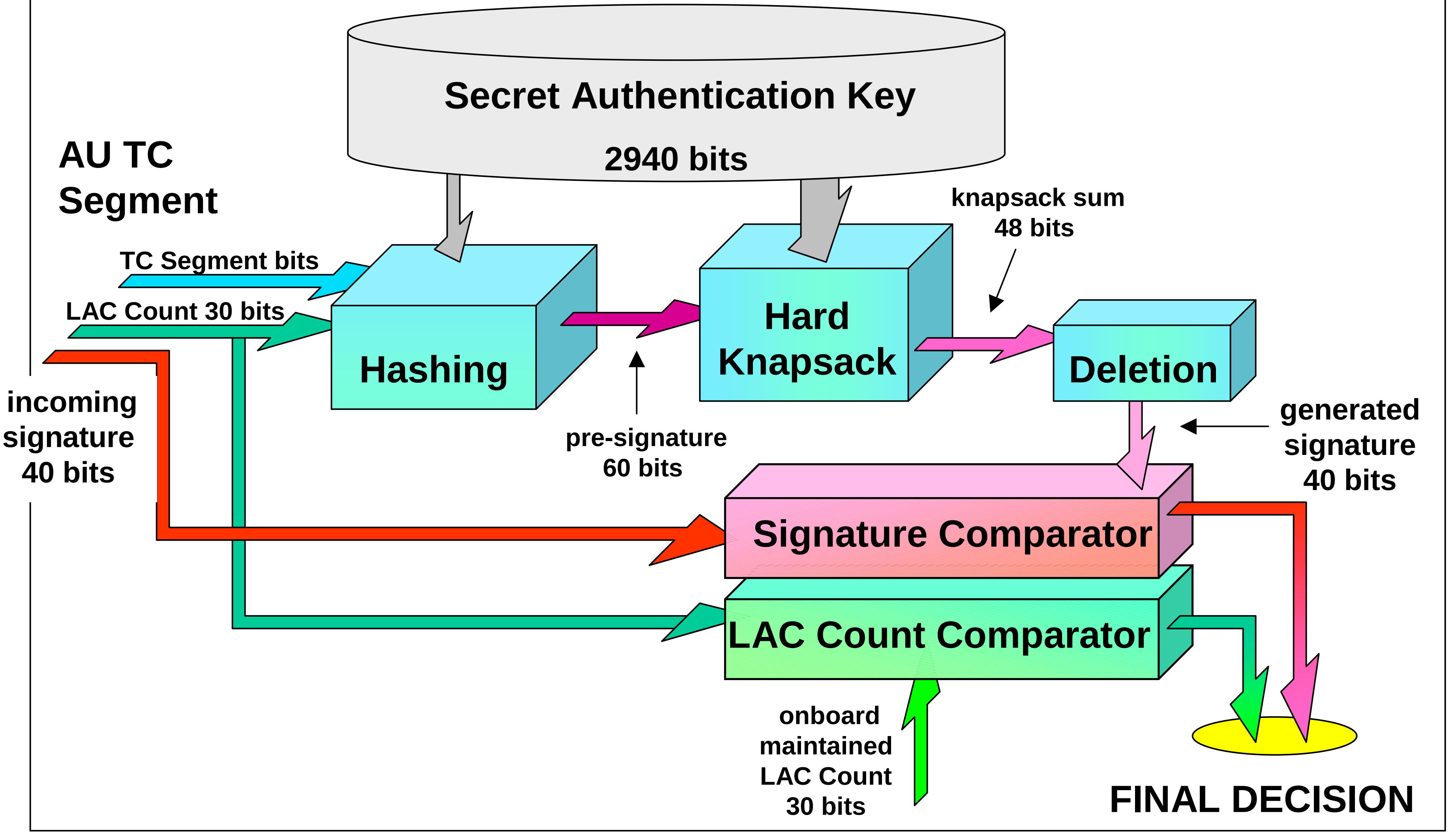
- 30-bit count incremented with every new TC.
- Input to the signature generation.
- Identical TC Segments have different LACs -> no ***replay attacks***
- 3 independent LAC Counts are maintained on-board, and ground:

  1 - **Principal:** nominal use, in-flight programmable
  2 - **Auxiliary:** nominal use, in-flight programmable
  3 - **Recovery:** emergencies, non-volatile, in-flight programmable

LAC ID:

- 2 bits indicating which LAC count is used

ESA Authentication Tail (2): The Signature



Secret Authentication Key

2940 bits

AU TC Segment

TC Segment bits

LAC Count 30 bits

incoming signature 40 bits

Hashing

pre-signature 60 bits

Hard Knapsack

knapsack sum 48 bits

Deletion

generated signature 40 bits

Signature Comparator

LAC Count Comparator

onboard maintained LAC Count 30 bits

FINAL DECISION

ESA AU Operational Aspects

In-flight Programmability & Test:

- 6 PSS defined *AU Control Commands* + 1 ¨Dummy¨ test command

- 2 types of *Authentication Key* :

  FIXED KEY: start-up/emergency phases, mission specific

  PROGRAMMABLE KEY: normal operation

- The 3 on-board *LAC Counters* can be set to any value

- AU can be switched on and off by “pulse commands”

AU Telemetry:

- FRAME ANALYSIS REPORT (FAR) : type of TC Segment (data,command,test) or rejection reasons.

- AU STATUS REPORT: actual value of the 3 LAC Counts on-board + Type of AU Key in use.

AUTHENTICATION vs. ENCRYPTION

R	O	D	O	T	A	N	X	S

D	T	A	R	O	O

Ensure intruder access denial	Ensure data confidentiality

Transformation Algorithms are public, Keys are secret, without the key, no acceptable TC can be generated

Data is visible, signature encrypted	**Data is hidden (encrypted)**
<u>One-way</u> transformation: different Keys, data fields, can yield same signature	**<u>Two-way</u> transformation: only one pair (Key,Plain text) can yield given cypher text**
Key robustness to hackers is not dependent on TC data contents	**Guessable data can help hackers break Key**
Replay attack is not possible	**Replay attack is possible**
Key can be changed, large (2940 bits)	**Key is fixed (3DES is 168 bits)**
Between Segmentation and Transfer L.	**Should be done At Application Layer**

AUTHENTICATION OVERHEADS

Space Segment

Ground Segment

ASIC: TC Decoder with built-in ESA compliant AU units are available since mid 90's (Dynex, Saab, Alenia)

Processor Board + **SW** : Key generation, AU Control, Signature generation and attachment

ROM: Fixed Key & Recovery LAC Count

RAM: Programmable Key + Principal and Auxiliary LAC Count

A sealed "***black-box***" automated system should insert AU sublayer ensuring safe and transparent Secret Keys' management by Ground Control Center

Conclusions

- **“Space Terrorism”** exists and cases could rise with the growing number of, not only military, but commercial and scientific S/C of high economical, social and/or political value.

- Any near Earth S/C is a relatively easy target of **impersonation attacks**, unless specifically protected.

- Plain ***encryption***, often confused with *authentication*, does not eliminate the risk of impersonation attacks. It should be managed by individual end users at Application Layer

- **ESA Authentication** provides effective, proven, low overhead protection against intruders’ TCs in the uplink.