SECURITY ASPECTS OF SPACE OPERATIONS DATA

Stefan Schmitz

TÜV Rheinland, Cologne, Germany

ABSTRACT

This paper deals with data security. It identifies security threats to European Space Agency's (ESA) In Orbit Infrastructure Ground Segment (IOI GS) and proposes a method of dealing with its complex data structures from the security point of view. It is part of the "Analysis of Failure Modes, Effects Hazards and Risks of the IOI GS for Operations, including Back-up Facilities and Functions" carried out on behalf of the European Space Operations Centre (ESOC).

The security part of this Analysis has been prepared with the following aspects in mind

- ESA's large decentralized ground facilities for operations,
- the multiple organizations/users involved in the operations and the developments of ground data systems, and
- the large heterogeneous network structure enabling access to (sensitive) data which does involve crossing organizational boundaries.

An IOI GS data objects classification is introduced to determine the extent of the necessary protection mechanisms. The proposal of security countermeasures is oriented towards the European "Information Technology Security Evaluation Criteria (ITSEC)" whose hierarchically organized requirements can be directly mapped to the security sensitivity classification.

1 SECURITY SITUATION OF THE IOI GS

The first consideration for the formulation of the security situation is the threats to which elements of the IOI GS are exposed. The threats are a function of the operational environment of the system and sensitivity of the data being processed in the various IOI GS facilities. The three basic security threats /ITSEC/ to which the facilities are exposed to are:

- the unintentional or unauthorized disclosure (loss of confidentiality),
- the unintentional or unauthorized modification (loss of integrity), and
- the unintentional or unauthorized destruction (loss of availability).

The causes of these threats are not only misuse. Weak points in the Information Technology, human failure, and acts of God are also essential reasons.

The threats can be of differing significance to different types of data. For example, for a flight element, the disclosure of operations commands represents little or no threat, while their modification can cause serious damage, at worst the physical destruction of the spacecraft and the death of the crew if more than one command was modified.

The second consideration would be the assessment of the materialization of these threats in the context of the IOI GS environment. Assumed impacts could be estimated in terms of

- loss/injury of human life
- destruction of/damage to material and/or equipment
- degradation of functionality
- delay of mission

as for example laid down in the ESA standard ESA PSS-01-40.

The problem lies now in the creation of appropriate IOI GS units (function, data, or facility), which enable the association with some sort of security classification. The solution of this problem would result in a categorization scheme for the selected IOI GS units. Such a categorization scheme would simplify the identification of weak points and allow the assignment and evaluation of countermeasures to reduce the security risk.

2. APPROACH ADOPTED

The approach adopted in this analysis is illustrated in *Figure 1*. It describes basically the method of categorizing data into sensitivity levels which are applied to the IOI operations systems. This includes the definition of data objects (for example Payload Experiment Results, Telemetry, Platform Operations Commands) used within the IOI GS. These data objects are associated with their environment so that it is possible to imagine potential threats and their materialization.

The worst impact assessment leads to one of five consequence classes (☞ chapter 4) for each of the analyzed data objects. Thus it becomes apparent

which data needs to be protected and which not. The results of this assignment are summarized in decision tables (☞ chapter 6).

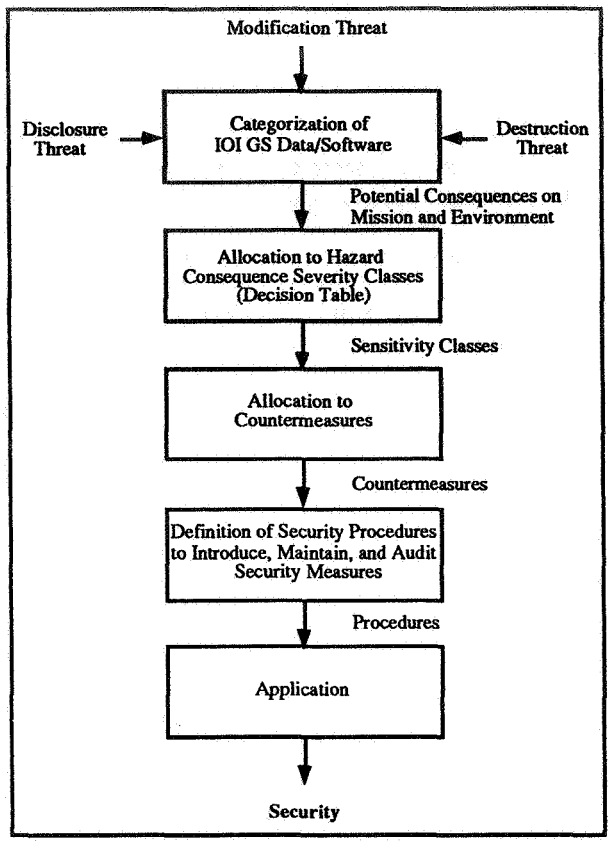

Figure 1: Approach Adopted

The sensitivity of the considered data object determines the effectiveness of the measure(s) to be implemented to counter the risk (☞ chapter 8 and 9).

3 SECURITY THREATS TO THE IOI GS

The security threats as pointed out above must be applied to all phases of the mission(s), including the preparation, the operation, and the maintenance. The following list of some of the most important threats is particularly related to the nature of IOI GS.

1. Introduction of unapproved codes during software development in terms of (non-) correctness and potential to be "infected". This is especially important due to the involvement of the large number of firms entrusted with the task of developing "ESA software".
2. As a result of the above mentioned point the access to confidential design documentation (hardcopies and on-line documents) by potential misusers is relatively easy.
3. The degree of decentralization of the Ground-Facilities-for-Operations (GFO) necessitates complex communication links between the centers, as well as within the centers and connected sites themselves. This complexity (large number of nodes to be interconnected) increases the opportunities for potential intruders to "break in" (for example in order to infect system software or to obtain secret experiment data from a user).
4. The large number of information sources necessary to operate the IOI facilities increases the probability of incorrect decisions based on illegally modified or unintentionally falsified information.
5. The architecture of the IOI GS control centers allows access to sensitive data from a number of different work stations for each (authorized) user. This creates strong demands on the data protection mechanisms against erroneous and unintentional manipulation of data.
6. The use of state-of-the art, ergonomically optimized Human Computer Interfaces (HCI) may also be useful for people having gained access to a computer for malicious purposes. Then the "help functions" could be too helpful.
7. The freedom of the User Home Bases (universities, research centers) to run their on board experiments (payload control, processing of experiment data) and develop their own on board software for this purpose involves the danger that the user's software cannot be controlled in the same way as ESA software. That means secure, software controlled operations are difficult to achieve.
8. The repeated updates/upgrades/ replacements required to be carried out on IOI and GS systems (by ESA as well as by users) call for security considerations of the same kind as the original development.
9. The maintenance of ESA data processing facilities through "outside" suppliers holds the danger of ease access to hardware, software components and critical data (for example replacing of harddisk, or software updates). This is specially important for re-arranging of system configuration or system adjustment. - If system changes can only be carried out by the supplier, a dependency in a very sensitive area arises.
10. For safety and availability reasons backup operations centers must be provided (for example having an additional stand-by control centers during critical operations). This further increases the security risk for data/software as well as for communications and people (see above).

4 CONSEQUENCE CLASSES

The first stage in the creation of security classes is the definition or application of some sort of consequence classes. Each piece of software or data can be associated with one of these consequences classes as-

suming the worst impact caused by the materialization of a potential threat. Based on ESA PSS-01-40 (Hazard Consequence Severity Categories) five security related consequence classes have been defined. They comprise in short:

1. CAT (Catastrophic): Loss of life, life threatening or permanently, disabling injury.
2. CRT (Critical): Temporary non-availability of some flight systems or some of its vital parts that could cause the failure of experiments.

In both cases, the only recovery is to abort the current mission.

3. MAR (Marginal): Temporary non-availability of some systems.
4. SQM (Subsequent Mission): No consequence for the current mission. Unauthorized use of data could compromise potentially future mission(s).
5. NEG (Negligible): Minor problems, without serious impacts on the mission.

5 DATA OBJECTS

A further step to reach a security classification is the definition of data objects used within the IOI GS. Taking into account the risks involved in the consequence classes described above, these data objects provide the basis for the worst impact analysis.

The following list contains the generic data objects for those pieces of data defined for the IOI GS:

- Crew Data
  - Medical Data
  - Voice/Video Data
- Platform Data
  - Commands
  - Telemetry
- Payload Data
  - Commands
  - Telemetry
- Experiment Data
- Ground Segment Data
  - Command Process-Line
  - Telemetry
  - Engineering Support, Test and Training
  - Characteristics Data Base
  - Reports
  - Experiment Data
  - Filed Experiment Data
  - Network and GFO Management Data

6 DECISION TABLES

Each of the above mentioned data objects (and the software which handle it) was evaluated in respect of the threats of disclosure, destruction, and modification bearing in mind the particular security situation of the IOI GS described in chapter 3. The results were summarized in tables of which one example is shown below:

SENSITIVITY CLASS	CAT	CRT	MAR	SQM	NEG
GS DATA					
Experiment Data ... 		mod/ des			dis

Table 1: Decision Table (Example)

Abbreviations of the considered threats as used in the tables:

- mod = modification (covert and open)
- des = destruction (both irretrievable destruction and temporary inaccessibility)
- dis = disclosure

The decision tables assign a sensitivity class to each data object. The class is derived from their Hazard Consequence Severity Category. Thus in the example shown in *Table 1* the "Experiment Data" is categorized as critical in the event of its modification and destruction (mod/des). The disclosure risk (dis) is negligible.

7 CRITICAL IOI GS DATA OBJECTS

The evaluation of the data objects has revealed that in the majority of cases the modification (covert and open) and destruction of data and software can have more serious implications on the mission and its environment than the disclosure risk. This finding should justify placing emphasis on the protection against the materialization of these kinds of risks.

Special attention must be paid to the very sensitive data objects, such as "PF operations commands", "system operational procedures", including their telemetry and the "network and GS management data". Their modification could result in catastrophic consequences. It is therefore important that these kinds of data are treated separately in relation to processing storage and transmission.

Another very sensitive type of data is that of "network and GFO management", since it contains all security implementation characteristics, such as compu-

ter hardware, software and network configurations or access control information. Hackers usually start by modifying this sort of data once they have "broken in". This provides them with the opportunity to continue with further (malicious) manipulations. So the administration of this data must provide a very effective mechanism to protect it against unauthorized disclosure.

In this context it is worthwhile noting that long term investigations carried out by security consultants dealing with a broad spectrum of customer establishments have found out that the most important threat of errors and omissions is caused by honest employees, who make mistakes in data entry, data update, changes in applications, etc.

8 COUNTERMEASURES

The main goal of the study is to describe a systematic method for identification of threats and the allocation of suitable countermeasures. The estimated degree of sensitivity of the threatened data object should determine the requirements on the systems to be designed.

A suitable means of achieving this goal is the use of the European IT Security Evaluation Criteria /ITSEC/ for two reasons:

1. They provide a basis for a standardized formulation of security aspects in the design documentation. That means Basic Security Functions as laid down in ITSEC:
   - Identification and Authentication,
   - Access Control,
   - Accountability,
   - Audit, and
   - Object Reuse

   are used accordingly to their ability to cover the actual threat(s) of each security relevant system to be analysed. In the same way the telecommunication security of all end-to-end telecommunication services can be examined by means of:
   - peer entity authentication,
   - access control,
   - data confidentiality,
   - data integrity,
   - data origin authentication, and
   - non-repudiation.
2. The security criteria give the sponsors valuable help for the formulation of requirements on and the Evaluation of Correctness and Effectiveness of the security characteristics. The ITSEC distinguish seven hierarchically structured Evaluation Levels. Each Evaluation Level defines assurance requirements with regard to
   the Correctness of
   - the Development Process (Requirements, Architectural Design, Detailed Design, Implementation),
   - the Development Environment (Configuration Control, Programming Language, Compilers, Developers Security),
   - the Operational Documentation (User Documentation, Administration Documentation), and
   - the Operational Environment (Delivery and Configuration, Start-up and Operation)

   and the Effectiveness of
   - the Construction (Suitability of Functionality, Binding of Functionality, Strength of Mechanisms, and Construction Vulnerability) and
   - the Operation (Ease of Use, and Operational Vulnerability).

The following table shows a possible assignment of the ITSEC Evaluation Levels to the Sensitivity Classes:

Evaluation Level	Sensitivity Level
E1	NEG
E2	SQM
E3	MAR
E3	CRT
E4	CAT

Table 2: Assignment of Evaluation Levels

The Correctness and Effectiveness requirements on the systems are suited to the sensitivity of the data they process. That means the quality of a security related system increases with the sensitivity of its data. For example the ITSEC require from E2 onwards, the support by a configuration control system, or from E4 onwards, a formally specified model of security.

TECHNICAL COUNTERMEASURES	CAT	CRT	MAR	SQM	NEG
System Software					
System Software should provide mechanisms for the handling of data of different sensitivity levels. It should contain the following basic security functions as integral parts:					
- identification and authentication	X	X	X	X	X
- access control	X	X	X	X	X
- accountability	X	X	X	X	
- audit	X	X	X	X	
- object reuse	X	X	X		

Table 3: Structure of Technical Countermeasures

TECHNICAL COUNTERMEASURES	CAT	CRT	MAR	SQM	NEG
Communication					
Use of secure/certified network or communication software and hardware preferably as integral part of the underlying operating system. In particular containing means for:					
- peer entity authentication	X	X	X	X	X
- access control	X	X	X	X	X
- data confidentiality	X	X	X	X	
- data integrity	X	X	X	X	
- data origin authentication	X	X	X	X	
- non-repudiation	X	X	X		
Data Bases					
Database(s) which administer for example the network management data, engineering support data, and characteristics data must be considered as very critical. The following set of exemplary security functions should be implemented:					
- identification and authentication	X	X	X	X	X
- administration of user, roles (user with special attributes), and process rights	X	X	X	X	
- access only possible using specially established processes	X	X	X	X	
- defining new types, granting or revoking access rights to existing types only by authorized users, initiated by this users via a trusted path	X	X	X	X	
- access to objects of certain types only via fixed established processes	X	X	X	X	
- verification of user roles, and process rights	X	X	X	X	
- auditing definition or deletion of types	X	X	X	X	X
- auditing granting or revoking of access rights for objects or object types	X	X	X	X	
- auditing remote data base access	X	X	X	X	

Table 4: Structure of Technical Countermeasures

A possible assignment of the functional requirements show *Table 3* and *4* for the areas of systems software (operating systems), data bases, and communications. The crosses in the right columns indicate merely that the functional requirements in the left column have to be implemented for a certain sensitivity class. For the Correctness and the Effectiveness of these requirements the hierarchy of ITSEC can be used.

These examples have a high abstraction level and give guidance for structuring requirements rather than providing them. More detailed specifications can be formulated such as in the following table:

TECHNICAL COUNTERMEASURES	CAT	CRT	MAR	SQM	NEG
Logical Access					
Automated audit procedure, allowing the supervision and control of resource usage. It should detect successful or attempted misuse of resources, software, and data. This requires the design of standardized audit interfaces to be implemented in each system (for example Workstations) to be monitored. Each system reports action to a centralized audit manager.	X	X	X		
...					
Measures against "hackers" and "crackers" for example:	X	X	X	X	
- avoiding naming of organization					
- avoiding identification of hardware					
- not using separate prompts for User Name, ID, and password					
- prohibiting message "Unauthorized Access ..."					
- protection of program code for example by:					
- submitting program to administration of access rights					
- frequent check of program size and creation date					
- not leaving sensitive data or software on the network if avoidable.					
...					

Table 5: Example of Security Requirements

9 ORGANIZATIONAL CONTROL

This chapter has been added to stress the fact that technical countermeasures alone, as raised in the pre

vious chapter, are insufficient to implement an effective security system.

A weak point is the users themselves: Many of them are unaware of the vulnerability of the data they operate with their systems. Highly sophisticated technical security measures can be useless, if users do not secure their working areas (for example simply by locking doors, log off the work stations from the network, or by mentally noting their passwords rather than keeping a written note on their desk).

Technical measures must therefore be complemented by organizational means, which control their implementation as well as ensuring their maintenance and development.

ORGANIZATIONAL CONTROL	CAT	CRT	MAR	SQM	NEG
Establish independent security staff with authority to act full time for the entire organization. This staff should be responsible for the following issues:	X	X	X	X	X
Check (screening) and selection of personnel corresponding to the task they are or will be entrusted with. For example, only well educated and experienced staff for development/ operation of critical software/data should be allowed. External personnel such as maintenance staff having access to data processing facilities and consequently to sensitive data as well as cleaning staff, plumbers, electricians (theft, espionage) must also be taken into account.	X	X			
...					
Programme to ensure security awareness of staff and users, including the requirement to sign a statement to acknowledge understanding of their responsibilities.	X	X	X	X	X
...					

Table 6: Complementing Organizational Measures

Table 6 represents a subset of lists of suggestions to be seen as counterparts to the tables containing the technical countermeasures. They serve as a possible input for the agency's security policy that in general constitutes the proceduralization of the technical security measures. Which one, or which set of the proposed procedures will finally be adopted in this security policy and the way of adopting them depends on the overall security architecture of the IOI GS.

From the organizational point of view data security is closely related to the Quality Management within an organization. That means, derived from a general security policy, procedures are implemented which ensure their introduction, maintenance, and ongoing development. These procedures are hierarchically structured in the same way as the technical countermeasures and reach to the project level. Their adherence and effectiveness must be audited in the same way as it is known from an effective Quality Assurance System.

10 CONCLUSION

The described procedure for the elaboration of a security concept can be applied to a lot of organisations which would certainly be worthwhile in many cases. Unfortunately security awareness arises only when something unexpected occurs (espionage, virus attack, failures, etc.).

The approach as described in this paper can prepare the ground for finding a way of improving security within an organization. The approach is based first of all on the definition of data objects, whose sensitivity determines the correctness and the effectiveness of the security enforcing functions and the extent to which organisational measures has to be complemented. In order to systemize the design procedure, proven standards can be applied.

This procedure only has a chance of success, if it is regarded as necessary by the management of an organisation and if the employees are motivated accordingly. Data security is an ongoing task and its efficiency depends considerably on how it is planned and supervised by the security staff.

11 REFERENCES

GISA1 German Information Security Agency (GISA)
Bundesanzeiger ISBN 3-8 88784-192-1
Criteria for Evaluation of Trustworthiness of Information
Technology (IT) Systems
1st Version, 1989

ITSEC Information Technology Security Evaluation Criteria (ITSEC)
Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom -
Version 1.2; Juni 1991