ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)
2.5 Safety and security of the ATM infrastructure :

METHODOLOGY FOR COMPUTER SECURITY IN OPERATIONAL NETWORKS OF THE FRENCH OFFICE FOR AIR NAVIGATION

(Presented by France)

SUMMARY

Computer systems have now taken a major place in air navigation, and their safety and security is vital to carrying out the tasks of air navigation services.

The purpose of this working paper is to present the methodology adopted by the French Office for Air Navigation to deal with the problem of the computer security of its operational information system.

Action by the Conference is in paragraph 5.

1. BACKGROUND: THE PROBLEM OF COMPUTER SECURITY AND SAFETY AT THE FRENCH OFFICE FOR AIR NAVIGATION

1.1 Maintaining an information system's safety can be defined in terms of ensuring its availability, integrity and confidentiality. Security, which may be considered as a subset of an information system's safety, is specifically aimed at protecting the information system's safety against malicious attacks.

Computer systems have now taken a major place in air navigation, and the safety and security of the information system is vital to carrying out the tasks of air navigation services.

Until a few years ago, the air navigation information system was closed and offered little or no interaction with the outside world. It had low vulnerability to security threats simply by virtue of the fact

that it was difficult to gain computer access to the information system from anywhere outside it. In such circumstances, **security** could be limited to protecting physical access to the information system.

1.2 For some years now, though, we have seen that while the importance of the information system to air navigation has grown, the system has progressively become more complex and is evolving into one that is increasingly interconnected with other systems and networks outside of the control of the air navigation service. This interconnectedness is necessary because of the need for interaction and data exchange with the partners of the air navigation services (European partners, airlines, etc.). At the same time, "proprietary" technologies are gradually losing ground to standard technologies such as the IP (Internet Protocol) for networks, or UNIX for operating systems.

All these factors make the information system more sensitive and increase the risk of exposure to external threats. The risk of security breaches of the information system by malicious parties thus increases significantly.

1.3 It thus became clear to the French Office for Air Navigation that it had to pay more attention to the problem of maintaining its information system security and safety, and specifically protection against external logical threats.

2. DEALING WITH THE PROBLEM

2.1 In order to be able to lower the information system's risk to an acceptable level, technical, organizational and procedural protection measures must be defined that are capable of correcting the information system's vulnerability. Such measures must be devised with rules that:

— address the problem exhaustively;

— define uniform protection measures;

— define protection measures that are applicable, recognized and are actually applied.

2.1.1 Addressing the problem exhaustively means that all aspects that may have an impact on security must be covered, including: the computer system's interconnection with the outside world, its internal interconnections (between sites), the use, operation and maintenance of computer equipment, technical and functional changes, the organization and responsibilities of human resources, and security incident or accident management.

To be exhaustive, the coverage must also take into consideration all the elements of the information system that have a "safety requirement" or for which a security breach can have an impact on the performance of air navigation tasks.

2.1.2 Protection measures must be uniform within the computer system. Indeed, the effective protection level of the computer system is only as good as its weakest link. It is thus futile to try to apply extremely cumbersome and costly protection measures to one part of the system if another part which is just as sensitive is left with little protection.

2.1.3 The protection measures must be applicable and must take into consideration the constraints and specific nature of the context. When drawing up security rules, the technology used, operational security constraints, users' and operators' habits and practices, etc. must thus be taken into consideration. Lastly, in order for these rules actually to be applied, it is imperative that they should be recognized by the computer system's operators and users, who must be familiar with them, and that they should be applicable in the same way as the already existing rules for system operation and use.

2.2 Taking into consideration all these factors, France has set out to formalize a high-level, general computer security policy. The project, called PSINA (*Politique de Sécurité Informatique de la Direction de la Navigation Aérienne*), aims to define general computer security rules for all the "operational" systems of air navigation that are part of the Air Traffic Control Information System (SICTA).

This general security policy should be reflected in a document with the following chapters:

— Objectives and limits of PSINA: Definition used for the information system, principles adopted, threats handled and the place of PSINA in relation to other existing rules;

— Classification of the information system's components: Four levels of sensitivity are defined for the functional and physical components of the information system, along with the criteria for classification of the components at the various levels. Classification takes place along three lines: availability, integrity and confidentiality;

— User access to the information system: rules for security clearance, for accreditation, for authentification, for traceability of actions and for use when external staff are employed at the Directorate General of Civil Aviation;

— Physical protection: rules for the protection of sensitive information media (removable or portable media, etc.), protection and physical location of computer systems;

— Maintenance and administration of the information system: rules for security clearance, for authentification of maintenance personnel, for employing external maintenance technicians, and for the traceability of system maintenance and administration operations;

— System interconnection and data exchange within the information system: adoption of "trustworthy areas" defining uniform security parameters and rules for the use of private and public networks for internal interconnection;

— Interconnection and data exchange with external entities: rules for accessing the information system from the outside and for having access to external entities from the information system, rules for the use of public or private networks for external interconnection, rules for issuing and receiving computer data between the information system and external entities;

— Evolution of the information system: a reassessment of component classification and of safety levels whenever the information system is modified; rules for the integration of new components or the withdrawal of old ones;

— Security incidents and accidents: definition of a security incident or accident, classification and detection of incidents, actions to be taken when a security incident is detected; rules for internal and external communication concerning security incidents and accidents; definition of principles for penalties and proceedings against malicious parties within and outside of the Directorate General of Civil Aviation.

— Organization of human resources related to information system security: user awareness of security/safety issues and awareness among decision-makers of security issues, authorization of "security" officials, security administration and maintenance rules, etc.

2.3 In order to ensure that the rules established under this security policy are applicable and that those involved in the information system are immediately familiar with them, a Working Group was formed and was assigned the task of drawing up a policy proposal. The Working Group is composed of representatives of the various operational air navigation services. Additionally, to ensure that PSINA is effectively recognized by the various operators and users, it will be adopted by a Supervisory Committee chaired by the Office for Air Navigation, thus ensuring that it is authoritative.

2.4 Some examples of security rules drawn up under PSINA are given below.

— Any interconnection with external systems must be formally authorized by the security officer on the basis of a security file that specifically mentions the results of a previously conducted risk study.

— Any interconnection with the outside must be technically verified. This is intended in particular to ensure that at any given moment only the services authorized for such an interconnection are accessible and that only authorized correspondents (users or systems) can use it, etc. Furthermore, the verification must also make it possible to ensure that only those technical services (such as network protocols) that are strictly required for the authorized functional services can be used through the interconnection.

— For the most sensitive elements of the information system, it is forbidden to establish any interconnection using public networks (RTC, Internet, etc.).

3. ENFORCEMENT STRATEGY FOR THE ADOPTED METHOD

3.1 Because of the scale of the PSINA project, and in order gradually to deal with all of its aspects, some priorities have been set among the objectives.

The first objective is to secure the perimeter of the air navigation information system so as to deal with external risks. This is done by defining the security functions and rules that must be enforced at the borders of the information system.

Once this perimeter is secured, it will then be possible to deal with internal security. The response to internal risks is much more difficult to define and the means required are much greater, as it is impossible to "block" the entire system; indeed, the information system must remain usable and efficient, and it is thus not possible to adopt protection measures as radical and relatively simple as those used against

external risks. That is one of the main reasons that it was decided to turn to this aspect after first dealing with external risks.

3.2 Through this sequencing of objectives, the final objective is to be able to provide "deep-seated" information system security, with a perimeter defence employing control and security technology acting on the networks and network interconnections and an internal defence mechanism employing security technology that focuses on the internal network and the systems themselves.

4. CONCLUSION

4.1 France is currently continuing work to define a first version of its computer security policy. A proposal for drawing up the first chapters as a cornerstone of this policy (policy objectives and limits, rules for classification of information system components) has already been drafted by the Working Group, which is now continuing its work on rules for interconnection with external entities. This first proposal will soon be submitted to the Supervisory Committee.

4.2 Once these first chapters are supplemented with the chapter on human resources organization and computer security, it will be possible officially to implement an initial version of the Air Navigation Computer Security Policy at the French Office for Air Navigation.

4.3 This is a long-term task requiring a sustained effort in order to achieve a comprehensive security policy that is commensurate with its objectives.

5. ACTION BY THE CONFERENCE

5.1 The Conference is invited to:

a) take into consideration the risks threatening air navigation computer systems;

b) draw up Standards and Recommended Practices (SARPs) to ensure computer system security; and

c) assign to a group of experts the task of producing a general guide to assist States in implementing their safety and security policy, for example in the form of a checklist indicating the points and questions to be addressed by a safety and security policy and the means with which to ensure computer system security.

— END —