Architecture of the Security Access System for Information on the State of the Automatic Control Systems of Aircraft

Arkady Isaakovich Frid, Alexey Mikhailovich Vulfin, Victoria Viktorovna Berholz, Dmitry Yurievich Zakharov, Konstantin Valerievich Mironov

Faculty of Informatics and Robotics, Ufa State Aviation Technical University (USATU), K. Marx Street 12, Ufa, 450008, The Republic of Bashkortostan, Russian Federation
frid.ai@net.ugatu.su, vulfin.am@net.ugatu.su, berholc.viktoriya@net.ugatu.su, zakharov.dju@net.ugatu.su, mironov.kv@net.ugatu.su

Abstract: This article discusses a problem of a secure access provision, via Web-service, to a database. Databases contain critical information about the parameters of the life-cycle of complex technical devices (CTD). Information life-cycle support (LS) of CTD provides access to a projects organization, production facilities, suppliers, service organization and the end users in long-term projects, which complex system projects actually are, at all stages of the device's life-cycle.

Keywords: data base; web application; secure access; telemetry; aircraft

1 Introduction

Prospects for the development of aviation technology are closely related to the information support of flights and the operation of aircraft and their subsystems. Digital control systems, with a distributed structure, with elements of artificial intelligence, are increasingly used. Wireless control systems are being developed for the exchange of information between the components of aviation systems. Such types of exchange are carried out by means of radio signals. This can also be applied to automatic control systems (ACS), with gas turbine engines (GTE) [1]. Thus, information from sensors of the engine operational process (telemetric information, TMI), can be accessed through the radio channel, the control actions generated by the calculator. These fundamental issues should be resolved during development a wireless ACS of GTE [2]:

- Ensure the effective transmission of radio signals and interference immunity of communication channels
- Working of information channels in real time
- Reliability of transmission (passing) of the signal on board
- Autonomy of the power supply of certain elements of the information channels

However, the list of issues that need to be discussed is much wider. For example, the if there is a danger of external intervention, the problem of information security will arise.

2 Problems of Telemetric Information Transmitting

The more that the information exchange infrastructure on board an aircraft is developed, the more questions arise, related to provision of noise immunity and integrity of information. If the issues of protection from interference are solved by well-tried methods (anti-jamming code, etc.), the provision of integrity requires non-trivial solutions, in some cases. Attackers can intervene in the flight control process or in the process of transferring and storing data on the current state of aviation equipment. This type of data is called telemetric information. Cases of such intervention are known. Current telemetry transmission systems demonstrate vulnerabilities that are sufficient, not only for the leakage of passenger and airline data, but also for altering the course of the aircraft [2]. For example, a study of ground-to-board communication systems showed that the ACARS system, despite its versatility and ubiquitous use, is vulnerable. If it is hacked with ADS-B, an attacker can gain access to the flight control system and download flight plans and detailed commands [3].

The traditional technical solutions are used on equipped air routes are completely unsuitable for hard-to-reach areas, sparsely populated areas, with an undeveloped land infrastructure.

At the same time, the real costs of maintaining existing TMI transmission systems are based on satellite communications and are quite large and makes its use, very problematic.

Aeronautical telecommunication systems are also not reliable, but the combination of SATCOM satellite communications and HFDL data transmission mode can provide a higher level of system reliability. However, issues of information security do not allow for the classification of such systems as “reliable” class TMI transmission systems. A successful attack can jeopardize the management of the satellite communication channels. They are used by the Future Air Navigation system, the Pilot Data Link Communications (CPDLC) controller, or the onboard

address and system communication system (ACARS). Despite detailed vulnerability analysis, researchers do not report on the technical means used to break into satellite communication systems [4].

Thus, there is a need to ensure the reliability of data transmission systems on the status of elements and subsystems of aircraft based on the application of modern (including intelligent) technologies for the protection and processing of TMI. Further consideration of issues of ensuring the reliability of data transmission systems on the state of aviation equipment, to the enterprise, will be carried out with reference to the CCD GTE.

At the stage of operation of aviation equipment, the actual task is to collect information on the actual state of operational product and transfer it to the developer enterprise. On the basis of such information support, the enterprise can develop additional recommendations on the technology for further operation of the product, make improvements to the technical documentation, implement a number of measures, that are aimed to improve operational characteristics. To collect and store this information, enterprises create databases. The information on the stage of operation of the products and aggregates, the results of equipment inspections, failures, etc. are collected and stored. Requirements for information management systems of the initial stages of operation for enterprises developing and producing ACS by aviation GTEs should include [5]:

1) Automatic recording of information transferred from service
2) Ensuring the integrity and consistency of data as it accumulates in the database
3) The ability to extract from the database, at any time and for a long time (up to30 years) and in any required query format.

This ensures the integrity and consistency of data that enters and stores in the database requires the development of special security measures.

The current stage in the development of on-board telemetry systems (BTMS) is characterized, firstly, by the large amount of data generated by the sensors of the equipment and other types of information sources [6], and secondly, by the need to eliminate errors associated with data transfer from instruments and all telemetry- and, thirdly, the need to auto-mate the processing of most of the information, including the work on decision-making. Therefore, the problem of transmission and analysis at ground-based service centers of operational parametric information collected by BTMS is urgent for solving the tasks of supporting the life cycle of the gas turbine at the stage of operation and maintenance. The main parameters necessary for the registration and reflection of such information in the database of the GTE status are:

- Where is the operation of the product
- Object on which the product is operated

- The total operating time - the time of operation of the product from the beginning of operation
- Operating time - the time of operation of the product with reference to a specific object
- A fixed event linked to the product (repair, malfunction)

To solve these problems, it is necessary to develop an automated information system (AIS), capable of being distributed in large areas, processing large amounts of information and capable of providing remote access to necessary data. The problem of providing secure access to a database containing critical information about the parameters of the life cycle of the CCD GTE is relevant and in connection with the entry into force of new documents in the field of technical control by FSTEC [6]. The issues of ensuring secure access to such databases were considered in [7, 8, 9, 10], but, without taking into account changes in the regulatory framework.

The article proposes the structure of the organization for receiving and storing data obtained from the operation sites of the SAU GTE units at the enterprise-developer. The proposed scheme allows providing secure access to a database containing critical information about the GTE being operated on the basis of a protected WEB application.

The purpose of this study is to improve the security of access to a database containing critical information about the operated gas turbine engine.

Proceeding from the set goal, the following task is formulated:

1) Development of the architecture of a secure WEB-application for access to the data-base of the AIS system for supporting the life cycle of the SAU GTD.
2) Analysis of the existing structure of the AIS supporting the life cycle of the SAU GTD.

AIS is a set of software and hardware needed to receive, store and process information,

AIS solves the main tasks associated with receiving telemetric information about the state of the SAE GTE. Telemetry data from the BTMS board is planned to be obtained in three different ways:

1) Directly from the side of the aircraft during the whole flight time. This method of data collection is of the greatest interest for the study, since the use of real-time monitoring technologies will allow a full (operational, searching and intelligent) analysis of the operability of the aircraft systems, crew condition and control of its actions directly during the flight. If there

are technical problems with any of the modules, the Engineers will learn about this in advance and will be ready to repair before the aircraft lands.

2) Devices for reading the event log from the sensors of the aircraft modules. When performing technical inspection and maintenance of an aircraft on the ground, devices of this type are read and stored on the status of the modules throughout the previous flight.

3) Entering events into the database manually. The operator processes the information and enters information through the web application.

In the second and third cases, information enters the database through a web application that is an insulating layer between external networks and the internal structure of the AIS, since access from the external network is one of the most vulnerable places of the system.

A typical scenario for using a database to store critical information involves its operation in an environment that is hidden from everyone except network administrators and database administrators.

The widespread use of cloud technologies, mobile devices, virtualization, the Bring Your Own Device (BYOD, personal devices for work) and various technologies for remote work leads to the erosion of traditional perimeter protection of the corporate network. With the expansion of ways to access corporate resources (DB), the network no longer has a single entry point [6]. In this scenario, the risks of information security are increasing, as the company provides more and more access rights to external entities, which may become an indirect reason for the intruder to gain access to the database server located in the internal network of the company. One of the solutions to the problem is the organization of access to the information stored in the database, using a web browser that interacts with the middleware of the company, that accesses the database.

Such access to the database can be limited by means of access control facilities and provided only to a few permitted roles. Thus, if an attacker can overcome the perimeter protection of the network and will be able to perform queries against the database, provided that he does not have an account with which one of these roles is assigned, the database will still be safe. This process simplifies access control and ensures that no user (including an attacker) can access the database directly, but only through an account that has an associated role.

3 Interaction between AIS and Web Application

Web application provides secure access to AIS. It is an intermediate link between the AIS and the client. It is connected to a client via internet and to AIS via

enterprise's local network. When a client refers to a web application service they believe they are working directly with AIS. [7] A general diagram of interaction between AIS and web application is shown in Figure 1:

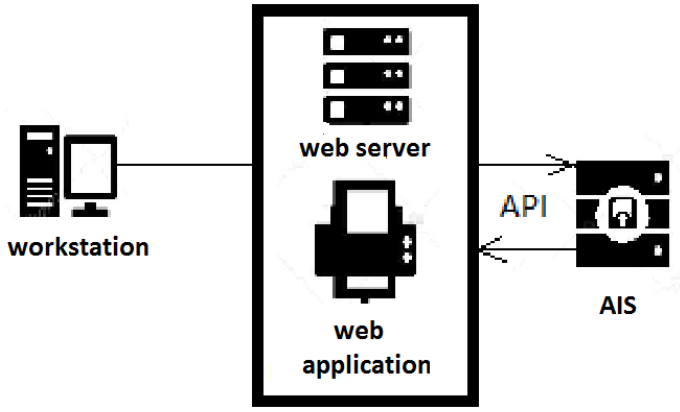

Figure 1
Interactions of the AIS and the web application

The Web Application is developed to make access to AIS more secure. It serves as a middle layer between user and AIS.

Web application provides access through 4 functions:

1. Identification
2. Authentication

   It is required to use two-way authentication, at the Web server level, to develop secure web application. Nowadays, the most secure technology of two-way authentication is authentication using Transport Layer Security (TLS) protocol.

   Using this technology requires a separate subdomain and configuring a Web server to work with TLS. Subdomain verifies a user's certificate. Server also must have a certificate that was certified by the certification agency.

   It is important to note that using a two-way authentication reduces probability of any type of attack. Two-way authentication occurs before user can open first HTML page. Thus, an attacker has no chance to interact with web application without a certificate. The attacker's actions will be stopped during the access to the web server by software which processes the connection. Therefore, web application will not even know about malicious actions.

After authentication at the TLS protocol level the server and the client begin to communicate through the user interface

3. Work providing by means of AIS

   It is necessary to restrict access to the AIS, the AIS access server and to local network by firewall. The firewall should be installed behind the outer. Such installation scheme creates a zone for the enterprise's local network enterprise and a demilitarized zone as shown in Figure 2.

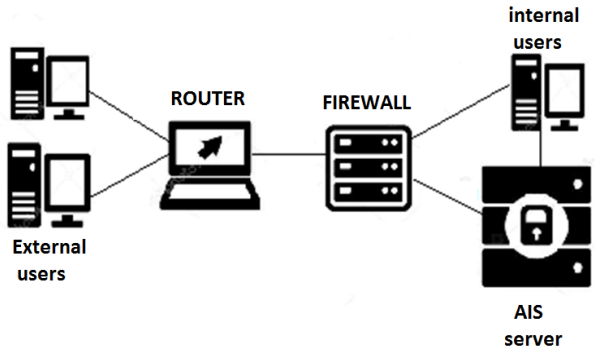

Figure 2
Wiring diagram of the firewall

4. Maintaining the History of Events

   Maintaining the history of events implies the following actions: generating event.

4 User Authentication Scheme at the Web Server Level using the TLS Protocol

It is required to use two-way authentication at the Web server level to build a secure Web application. It is required to build a separate subdomain, that will provide a user's certificate verification. Also, it is required to use a web server configuration that works with TLS. The web server should have a certificate.

The user authentication process at the web server level, according to RFC 5246 (The Transport Layer Security Protocol Version 1.2), is presented as a UML activity diagram in Figure 3 [8].

Two-way authentication occurs before the user can open the first HTML page. Thus, an attacker has no chance to interact with the web application without a certificate [9]. The attacker's actions will be terminated during the access to the

web server by the software that processes the connection. Therefore, the web application will not even be aware of the malicious actions.

After authentication at the TLS protocol level, the server and the client begin to communicate through the user interface.

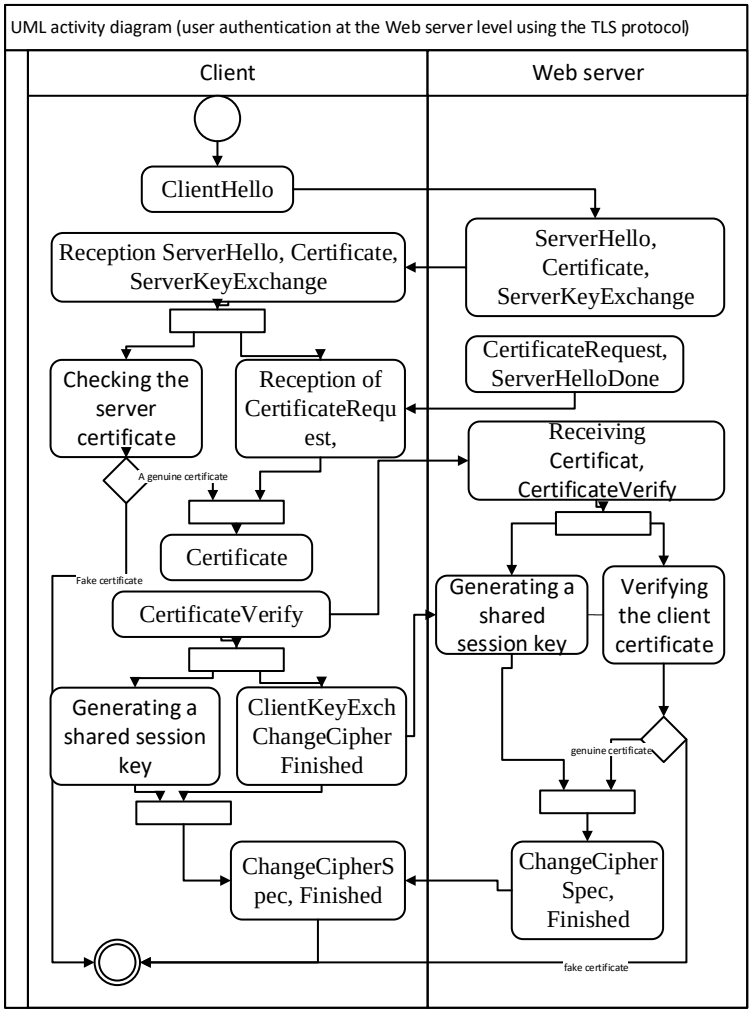

Figure 3
User authentication process at the Web server level

5 User-Level Authentication Scheme at the Application Level

The server and the client begin to communicate through the user interface after authentication at the TLS protocol level. The process of user authentication in the system (at the level of application logic) is presented as a UML activity diagram in following figure:

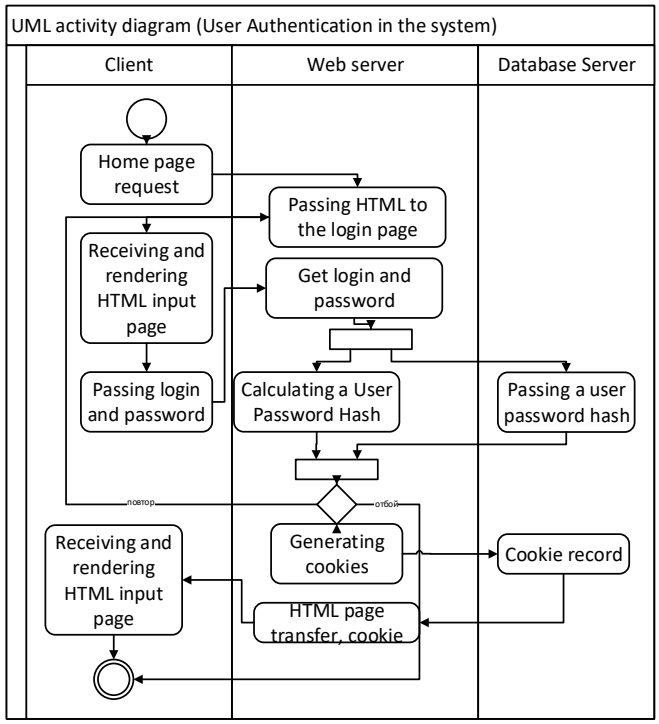

Figure 4
The process of user authentication in the system

6 The Scheme of Processing Requests from Remote Clients

The user can continue to work with the server. Authentication is at the web application level. It becomes possible because the cookie contains the identifier of the valid session. The process of processing user requests is presented in the form of the UML activity diagram, in Figure 5.

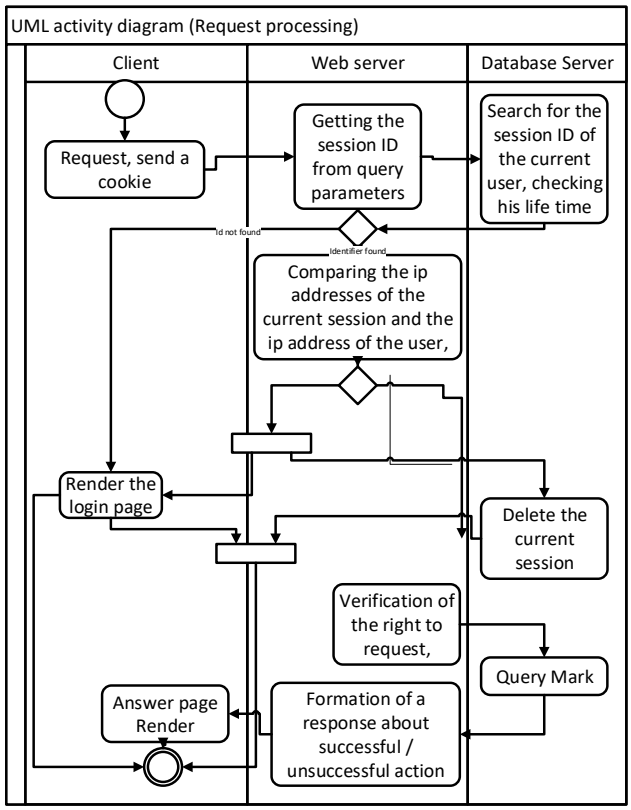

Figure 5
The process of processing user requests

7 Logical Data Model

In the process of developing the architecture of the web application, taking into account the general security requirements and requirements related to countermeasures against attacks on attacks, a scheme for application data was developed.

When analyzing all requirements, 5 entities were identified. Each entity and each data field has a semantic load and is introduced to provide the functionality of the application:

1) Users - an entity that stores user data associated with its identification and authentication. Fields of the entity:

a) user id - unique user identifier

b) email - the user's mail, a unique field on which it is possible to uniquely identify a user in the AIS. This field is also used to recover the password

c) encrypted_password - password hash of the user. The field is necessary for the requirement of secure data storage and the operation of the authentication algorithm

d) reset_password_token - a one-time token of the application for password recovery, which can be sent to the user's email account upon password recovery

e) reset_passwd_sent_at - time of creation of the previous field

f) sign_in_count - the field containing the number of moves of the user to the system

g) current_sign_in_at - the field containing the date and time of the current logon

h) last_sign_in_at - the field containing the date and time of the last logon

i) current_sign_in_ip - the field containing the current ip address

j) last_sign_in_ip - the field containing the ip address at the last login

k) failed_login_count - the field storing the number of failed inputs in a row

l) status - the field for storing the user status (active, blocked, the password reset is expected)

m) name - the field containing the user name

2) Roles - an entity necessary for grouping several actions with the subsequent assignment of action groups to specific users. Fields of the entity:

a) id-unique identifier of the role

b) name - the name of the role (for example, administrator, operator, extras, etc.)

3) User roles (UserRoles) - a table for communication between users and roles. Fields of the table:

a) id - identifier of the user role

b) user_id - user identifier

c) role_id is the role identifier

4) Actions - an entity that describes the actions that can be performed with a specific re-source:

a) id - the identifier of the action

b) api_url - url of the resource

c) methods - methods that can be implemented by an action

d) role_id is the role identifier

5) History - the entity for storing data about user actions:

a) id - the identifier of the history record

b) created_at - the date the record was created

c) user_id - user identifier

d) action_id - identifier of the user action

e) data - data that the user transmitted during the execution of the action

f) status - the status of the operation

For the interplay of the essence there were wings with each other by the following connections:

1) User - role - many to many

2) Role - action - one to many

3) Action - history - one to many

4) User - history - one to many

Conclusions

The anticipation of vulnerabilities in the WEB-application was carried out through the implementation of measures for the development of secure software, established by GOST R ISO / IEC 12207.

Modelling of security threats and detected vectors of possible attacks, as well as, their analysis, allows for the formulation of countermeasures for each of the vectors at the different architectural levels of the web application.

Countermeasures and indications to use protection technologies, with respect to the specific features of the architecture of the projected web application based on the Model-View-Controller pattern [10], made it possible to increase the safety of the use of AIS.

Therefore, increasing the security of access to a database containing critical information about the operated CCD GTE is based on the development of a secure web application architecture, that serves as an isolating layer for external AIS clients, which allows for the provision of transmission and analysis in ground service points of the operational parametric information, from the aircraft board and to provide the possibility of remote access to essential data.

Acknowledgement

This article is supported by RFBR grant № 20-08-00668

References

[1] O. S. Gurevich. Prospectives for the development of the SAU GTE in the work of the CIAM SSC / Abstracts of the International Scientific and Technical Con-ference "Aviadvigateli XXI Century" Moscow, CIAM, 2010, p. 838

[2] O. S. Gurevich, A. S. Trofimov, M. G. Kesselman, V. I. Chernyshov, A. A. Semin. Wireless Demonstration Control System for GTE / Abstracts of the International Scientific and Technical Conference "Aviadvigateli XXI Century" Moscow, CIAM, 2010, p. 812

[3] Mohsen Riahi, Manesh Naima Kaabouch Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system International Journal of Critical Infrastructure Protection, 2017, Vol. 19, pp. 16-31

[4] Mohamed Slim Ben Mahmoud, Alain Pirovano Nicolas Larrieu Aeronautical communication transition from analog to digital data: A network security survey, Computer Science Review, Vol. 11-12, pp. 1-12

[5] G. I. Pogorelov, Yu. O. Bagaev. Features of the management of logistics and parame- ter data of the SAU GTE at the initial stages of operation / Abstracts of the international scientific and technical conference "Aircraft engines of the XXI century" Moscow, CIAM, 2010, p. 777

[6] E. Naderi, K. Khorasani Data-driven fault detection, isolation and estimation of aircraft gas turbine engine actuator and sensorsm, Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on, 2017, web [http://ieeexplore.ieee.org/document/7946715/] 10.10.2017

[7] E. Naderi, K. Khorasani Data-driven fault detection, isolation and estimation of aircraft gas turbine engine actuator and sensorsm, Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on, 2017, web [http://ieeexplore.ieee.org/document/7946715/] 10.10.2017

[7] Gerald Beuchelt Securing Web Applications, Services, and Servers Computer and Information Security Handbook (Third Edition) 2017, pp. 183-203

[8] T. Premalatha, S. Duraisamy A certificate based authorization and protected application layer protocol for IoT, Computer Communication and Informatics (ICCCI), 2017 International Conference on, 2017, pp. 1-5

[9] HassinaNacer, NabilDjebari, HachemSlimani, DjamilAissan A distributed authentication model for composite Web services, Computers & Security, 2017, Vol. 70, pp. 144-178

[10] S. S. Hasan, R. K. Isaac An integrated approach of MAS-CommonKADS, Model–View–Controller and web application optimization strategies for web-based expert system development, Expert Systems with Applications, 2011, Vol. 38, pp. 417-428