Analysis of the methods of constructing information attack models for the system of telemetric information transmission

A.I. Frid
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: frid46@mail.ru

A.M. Vulfin
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vulfin.alexey@gmail.com

V.V. Berkholts
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: torina4@yandex.ru

Annotation

This article observes methods of information security risk assessment. Risk assessment is needed to build secure information system of receiving and transmitting telemetry data from the board of an aircraft. Here are analyzed models of attacks on information system. Time quantization was chosen as a main option of the risk assessment system.

1. Introduction

Modern aviation systems are complex hierarchical computing structures. The flight is carried out with permanent communication with ground control points. The flight requires two-way exchange of large amounts of information, including data from various aircraft sensors.

Ensuring the information security of telemetry information (TMI) transmission systems from the aircraft is a primary goal. Malfunction and dangerous state of the aircraft on-board equipment can be diagnosed by specialists of ground services. It allows to prepare for the repairing before boarding the aircraft. However, current TMI transmission and processing systems have vulnerabilities that can be exploited by intruders to gain access not only to passenger and airline data but also they can significantly affect flight parameters.

It is necessary to have models that allow the development of security analysis systems (SAS) during the design and operation phases. SAS operates a model of the analysed system based on the network specification and implemented security policy. As a result of the security analysis the vulnerabilities of the system are determined, the graphs of possible attacks are constructed and security metrics are calculated. This forms an integral assessment of the overall security level of the system as well as the security level of its components.

The results of the analysis make it possible to develop valid recommendations for the elimination of identified vulnerabilities. It ensures the required level of security of the system at all stages of its life cycle. Analysis system for the collection and transmission of telemetry data protection on the status of the on-board aircraft systems should be a hierarchical set of models:

• model of the attacker's behaviour;

• a model of attacking an attacker's actions aimed at implementing threats to information security taking into account his skills;

• model of vulnerabilities of the system;

• model for calculating system security metrics and a model for estimating the overall security level of the system.

There are many ways to analyze the flow and the probability of attack on information system, for example [1,2]. The range of indicators and criteria used for risk assessment is very wide. Mathematical devices used for risk assessment also vary. The methods chosen for the analysis of security are combined by the presence of a graphical representation of the attack flow and a probabilistic approach to risk assessment. Such diversity makes the choice of means of calculating the risk for the CAS system of receiving and transmitting telemetric information difficult.

The purpose of this paper is a comparative analysis of the methods for constructing intruder's actions model. To achieve this goal, it is necessary to solve the following tasks:

1. Analyze the life cycle of an attack

2. Analyze approaches to building attack models

Proceedings of the 6th All-Russian Scientific Conference "Information Technologies for Intelligent Decision Making Support", May 28-31, Ufa - Stavropol, Russia, 2018

2. The life cycle of an attack.

An attack is a set of intruder's actions leading to damage the information system's security. [3]. As a result of a successfully implemented attack the intruder can, for example, gain unauthorized access to information stored in the information system, disrupt the system's operation or distort the contents of the information system's data. The potential targets of the attack may be servers of the information system for the collection of telemetric information, workstations of operators of ground service stations or communication equipment [4].

A typical scheme of an attacker's actions according to [5] includes six steps:

Step 1. Intelligence activity.

The attacker identifies potential targets that satisfy his mission (for example, a failure of the TMI transmission, falsification of the sensor readings in order to hide the breakdown of onboard equipment peeling in order to know the position of the board in the air, etc.).

Step 2. Initial implementation

An attacker bypassing perimeter protection accesses the internal network through a compromised system or an operator account that processes data from the aircraft in real time or enters data into the system at the ground support station.

Step 3: Management and control.

The device compromised in the second stage is used as a bridgehead in the enterprise so that attackers can establish permanent, long-term and remote access to the information system of the enterprise that accepts TMI.

Step 4: Lateral movement

Once an intruder has an established connection to the internal network he seeks to compromise additional systems and user accounts. Since an attacker often pretends to be an authorized user in our case a ground service station operator or an enterprise engineer monitoring the condition of the aircraft, evidence of its existence may be difficult to access.

Step 5: Achieving the goal

At this step an attacker typically has multiple remote access points and can compromise multiple internal systems and user accounts.

Step 6: Final step

The attacker achieves the goal of his attack, for example, gets the opportunity to substitute data from the airborne sensors.

Paper [6] provides an example of managing the threat lifecycle. Here the life cycle of the threat is divided into 3 components: preparation, attack itself, consequences. The above steps 2-5 are integrated into one. It is necessary not only to detect and block the attack to analyze the security of the system for receiving and transmitting information.

Life Cycle Management of attack involves preparatory actions before the intruder attacks the enterprise. It also involves actions to compensate for the damage caused by the attack. For example, the following steps were proposed by the authors in [7] for the system of receiving and transmitting telemetric information:

1.Before the alleged attack: separation of access to the Web application, introduction of role-playing policy, fencing the enterprise network using a firewall.

2.During the attack: control of information leakage through the Web application, scanning of incoming Web traffic.

3.After - the mechanism of retrospective analysis, scanning of all outgoing traffic in search of already occurred infections.

It is necessary to develop methods for detecting attacks and protecting against attacks on computer systems and networks to build a secure system for the reception and transmission of telemetric information (TMI) from the aircraft

Such system implies different ways of transferring TMI to a ground receiving point of information:

Broadcast data from the board directly during the flight in real time.

Reading from the sensors using the IEEE 802.15.1 protocol of the device at the ground service station of the aircraft (LA)

Entering data from sensors by the operator manually.

The first method of transmission represents the greatest risk. If the attacker manages to attack the transmission channel from the aircraft and counterfeit TMI the damage caused by such an action can be catastrophic: incorrect data from sensors, concealment of aircraft damage, interruption of communication with the aircraft, access to the aircraft's geo position for physical attack, etc. Thus, the criterion for the time of detection of such an attack is the most essential for choosing a model for detecting attacks on the TMI reception and transmission system.

Attack models allow you to accurately determine the effectiveness of protection against simulated information attacks. An essential criterion for will be the possibility of the model being developed to quantize the course of the attack in time for constructing a model of attack on the computer system (CS)

Different ways of representing attack scenarios and building attack graphs (trees) are used in scientific studies to analyse security: attack trees, formal grammars, painted Petri nets. Next, some of the existing models of building an attack will be considered.

Attacks trees

This model was presented by B. Schneier [8.].

As a basic construction here is a hierarchical tree G = (L, E), where L = {li} is the set of vertices of the tree, E = {es} is the set of tree arcs. Each vertex of the tree G is

associated with a certain attacker's action. The root of the tree denotes the ultimate goal of the information attack, the implementation of which can cause significant damage to the CS.

Thus, it is possible to compose the set of possible paths Gp on the graph G where each path is a sequence of arcs. As a starting point of the path can act leaves of the tree G and as the ultimate apex - the root of the tree G.

This model of information security threats is constructed in terms of the mathematical apparatus of the theory of trees.

It allows to simulate complex attack scenarios that involve several implementation options. One of the essential parameters that can be calculated is the average time of the entire attack tree implementation. The average implementation time is related to the time of implementation of actions to implement the stage of the information security threat.

The most common are attack patterns based on graphs. The most well-known are attack graphs, Bayesian networks, Petri nets, and various extensions of these formalisms.

Attack graph

A graph of attacks is a graph containing all known trajectories (scenarios, paths) of the intruder's implementation of threats (goals). Each path in an attack graph shows a way in which an intruder can compromise the security of a system [9]. An analysis of such a graph can be performed to solve the following tasks: analysis of incidents; detection of possible attacks that are not detected by real-time attack detection systems. The key problem of building an attack graph for large networks is the scalability associated with the formation of an attack graph for networks with a large number of hosts and vulnerabilities. Charts of network attacks represent a set of possible scenarios of penetration into the computer network. Each penetration is a scenario - a sequence of actions taken by an intruder.

The attack graph can automatically generate attack paths for network vulnerability analysis. It can show users a weak point in the network analysis process for analysing the risk of network security. When a potential attack path is found attack graph tools can generate an attack schedule or attack trees to help system administrators understand how attacks occur and then take protective measures. Hypothesis analysis can be used in the attack graph to test the reliability of network configuration security and thus to protect unknown threats. However, there are difficulties in generating and visualizing attack building methods, such as the explosion of the state space, the high complexity of algorithms that are difficult to graphically demonstrate.

However, graph attacks are not adapted for ongoing attacks because they cannot represent the progression of an attacker nor be triggered by alerts. Thus, they must be enriched to provide the functionalities needed to perform Dynamic Risk Assessment, for example using Bayesian networks.

Bayesian attack graphs

An example of simulating attacks using Bayesian networks is Bayesian attack graphs, which are directed acyclic graphs. Vertexes are associated with incidents. The ribs model a conjunction or disjunction of elementary conditions [10].

It is based on a Directed Acyclic Graph where nodes represent random variables and edges represent probabilistic dependencies between variables [11]. For discrete random variables, these dependencies can be specified using a Conditional Probability Table associated with each child node. Bayesian networks are particularly interesting for computing inference, i.e. calculating the probability of each state of all nodes of the network, given some evidences, i.e. nodes that have been set to a specific state

To calculate the probability of occurrence of an attack or an incident under the condition of occurrence of previous incidents one can use the conditional probability formula. Advantages and disadvantages of Bayesian attack graphs are the same as the attack trees considered earlier. However, unlike attack trees, Bayesian attack graphs have additional advantages, as they are probabilistic models that allow for the case of uncertainties in the initial data about simulated attacks.

Among the varieties of Bayesian networks, it is necessary to identify hidden Markov models that are often used in attack modelling because of the convenience of investigating paths in the state space each of which is characterized by a given probability. This extension of Bayesian graph of attack is good for modelling zero-days attacks [12].

Petri nets are one of the widely used formalisms in simulating attacks in computer networks.

Comparison of toolkits for building attack graphs

Here is presented a table 1 which contains most-known toolkits for building attack graphs. The comparison is based on the following properties:

1. Openness of the resource. This property will allow us to use this product in further studies

2. Possibility of addition and expansion.

3. Characteristics of the attacker. This property is necessary for determining and separating the attacker's types and the complexity of the attack on the enterprise.

4. Discretization of the attack in time. As mentioned before, the time characteristic of the attack is necessary for us to assess the level of SAZ security.

5. Risk assessment form

.

Table 1. Comparison of toolkits for building attack graphs

Product / Feature	Open source	The possibility of additions and extensions	Characteristics of the attacker or level of attack complexity	Discretization of the attack in time.	Risk assessment form
Attack trees 1. Attack tree tool	no	no	attack complexity	no	Probabilistic
2. The SecurITree	no	no	attack complexity	no	Probabilistic
Attack graph 1. MulVal	yes	yes	attack complexity	no	Probabilistic
2.NetSpa	no	no	attack complexity	no	Probabilistic
Bayesian attack graphs 1.Bayesian Attack Model	no	no	attack complexity	No, but there is a dynamic risk assessment	Probabilistic

Conclusion

Analyzed modeling techniques attacks on the IS in theories suggest quantization timing attack, but none of the analyzed program complexes for constructing graphs attack does not possess such a characteristic. The most appropriate method is Bayesian graphs of attacks with dynamic risk assessment. Attack graphs and attack trees offer a static risk assessment for the system being designed. Dynamic risk assessment allows to obtain a probabilistic estimate of the risk of a specific attack in real time. Unfortunately, none of the products developed on the basis of this methodology exists in the public domain.

Thus, a further step in the design of a risk assessment system for the TMI transmission and reception system is the construction of a Bayesian graph of attacks with dynamic risk assessment.

Acknowledgments

This article is supported by RFBR grant № 17-07-00351

References

1. 1. MulVal Internet resource [http://people.cis.ksu.edu/~xou/mulval/]
2. TVA Internet resource [http://csis.gmu.edu/TVA/]
3. GOST R 53114-2008 Information protection. Ensuring information security in the organization. Basic terms and definitions
4. S.A. Nesterov Analysis and management of risks in information systems based on Microsoft operating systems
5. The six stages of a cyber attack lifecycle Internet resource [https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle]
6. Alexey Lukatsky A new model of information security taking into account the life cycle of an attack, Internet resource [https://gblogs.cisco.com/en/bda/]
7. A. I. Frid; V. V. Berkholts; N. Ju. Grebnev, Providing of the secure access to the complex technical device, the ICICAM, 2017, Internet resource [https://ieeexplore.ieee.org/document/8076398/]
8. B. Schneier Secrets and lies. Data security in the digital world St. Petersburg: Peter, 2003 - 367 s
9. S. Jha, J. Wing, R. Linger, and T. Longstaff. Survivability analysis of network specifications. In Proceedings of the International Conference on Dependable Systems and Networks, Workshop on Dependability Despite Maliciowns FauIts, New York, NY, June 2000.
10. Nayot Poolsappasit; Rinku Dewri; Indrajit Ray Dynamic Security Risk Management Using the Bayesian Attack Graphs of the IEEE Transactions on Dependable and Secure Computing, Vol. 9, Issue: 1, pp. 61 - 74
11. Aguessy, F., Bettan, O., Blanc, G., Conan, V., & Debar, H. (2016). Bayesian Attack Model for Dynamic Risk Assessment. CoRR, abs / 1606.09042.
12. hu, Zhisheng & Zhu, Minghui & Liu, Peng Online Algorithms for Adaptive Cyber Defense on Bayesian Attack Graphs. Proceeding of MTD'17, October 30, 2017, pp. 99-109