International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 18-23

Security Models

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *The range of reasons for unauthorized use of the system is wide enough: from the excitement of playing with a computer to the feeling of domination over a disgusting manager. This is true not only for amateurs who want to have fun, but also for professional programmers. They obtain the password by choosing, guessing, or sharing it with other hackers. Some of them not only browse the files, but also become interested in the contents of the files. This is a serious threat, as it will be difficult to distinguish indulgence from malice.*

Keywords: supply, model, category, ideological, unreliable, resource, disruptive, range, goal, target, security models.

INTRODUCTION

1. Information security intruder model

2. Harrison-Ruzzo-Ulman discretionary model

3. The mandated model of Bella-LaPadula

4. Security role model

1. Information security intruder model

To prevent potential threats, it is necessary not only to protect and control the use of operating systems and software, but also to identify the category of intruders and the methods they use.

Depending on the causes, purposes and methods, information security breaches can be divided into four categories:

- adventure seekers;

- ideological hackers;

- hackers-professionals;

- unreliable employees.

The adventurer is usually young, often a student or high school student, and rarely has a well-thought-out attack plan. He chooses his target at random, retreating when faced with difficulties. Such an adventure seeker shares his success only with close friends and colleagues.

An imaginary hacker is also an adventurer, but more skilled. He chooses specific targets (hosts and resources) based on his beliefs. His favorite type of attack is to change the information on the Web server or, in rare cases, to block the attacking resources. Ideal hackers for adventure seekers announce their success to a wider audience, usually by posting information on a hacker Web site or at a Usenet conference.

The hacker has a clear plan of action and allocates certain resources. His attacks are well thought out and usually take place in several stages. It first collects initial information (type of operating system, services provided, and security measures applied). It then plans an attack based on the information gathered and selects (or even develops) the appropriate tools. He then launches an attack, obtains confidential information, and finally destroys all traces of his actions. Such an attacking professional is usually well-funded and can work alone or on a team of professionals.

An unreliable employee creates the same problem as an industrial spy. On top of that, it is more difficult to determine its existence. It also has to remove the internal protection of the network, which is usually less robust, rather than the external protection of the

network. However, in this case, the risk of unauthorized use of corporate information is higher than that of a person with any other malicious intent.

METHODS

Figure 20.1. Model of information security intruder

The range of reasons for unauthorized use of the system is wide enough: from the excitement of playing with a computer to the feeling of domination over a disgusting manager. This is true not only for amateurs who want to have fun, but also for professional programmers. They obtain the password by choosing, guessing, or sharing it with other hackers. Some of them not only browse the files, but also become interested in the contents of the files. This is a serious threat, as it will be difficult to distinguish indulgence from malice.

Until recently, there were concerns that dissatisfied officials would abuse the position, disrupt the system, allow outsiders to use it, or leave the system unattended. The reasons for such actions are:

- reaction to harassment or reprimand by the leader;

- protest against non-payment of the company for overtime work;

- bad intentions such as retaliation in order to weaken the firm as a competitor to a newly formed firm.

Dissatisfaction with the boss poses one of the biggest threats to the user's computer systems. That's why anti-hacking agencies are dedicated to personal computer owners.

2. The Harrison-Ruzzo-Ulman discretionary model

As you know, security policy is a general definition of information processing it is understood that a set of procedures and rules, the implementation of which provides protection against a certain set of threats and is a necessary (sometimes sufficient) condition of system security. The formal expression of a security policy is called a security policy model.

Manufacturers of secure information systems use the security model in the following cases:

- development of a formal specification (detailed list) of the developed system security policy;

- in the selection and justification of the basic principles of the architecture of the protected system, which determine the mechanisms of implementation of protection measures;

- in the process of analyzing system security as a reference model;

- confirming the characteristics of the system, which is produced by formal proof of compliance with security policies.

By creating formal security models, consumers will be able to communicate their requirements to manufacturers in a clear and unambiguous manner and assess the suitability of protected systems for their needs.

Qualification experts use the security model as a benchmark when analyzing the adequacy of security policies in protected systems.

The security model is based on the following basic assumptions.

1. A system consists of a set of interacting "subjects" and "objects". Objects can be intuitively thought of as information containers, and subjects can be thought of as executable programs that affect objects in a variety of ways. In such an understanding of the system, the security of information processing is ensured by addressing the issue of subject management of the use of facilities in accordance with the set of rules and restrictions that form the security policy. The system is considered secure if the subjects are not able to violate the rules of the security policy. It should be noted that the definition of “object” and “subject” can vary significantly in different models.

2. All interactions in the system are modeled by establishing certain types of relationships between subjects and objects.

3. All activities are monitored by the interaction monitor and are prohibited or permitted in accordance with the rules of security policy.

4. The security policy is given in the form of rules, according to which all interactions between subjects and objects are obligatory. Interactions that violate these rules are prevented by means of use controls and cannot be carried out.

5. A set of subjects, objects, and the relationships between them (established interactions) determine the "state" of the system. Each system condition is safe or unsafe according to the safety criteria suggested in the model.

6. A key element of the security model is the proof of the theorem that a system in a safe state cannot become dangerous if all the rules and restrictions are followed.

The Harrison-Ruzzo-Ulman discretionary model is a classical discretionary model that provides for the voluntary management of the use of objects by subjects and the control of the distribution of rights of use.

In this model, the information processing system includes information-using subjects (S set), objects with protected information (S set), and corresponding actions (e.g., reading (R), writing (W). , is represented by a finite set of access rights representing the program execution (E)) vak = $\{r1, r2,\ldots, rn\}$.

Thus, the Harrison-Ruzzo-Ulman discretionary model does not guarantee system security in the general flow, but it is this model that serves as the basis for a whole class of security policy models that are used in all modern systems to manage access and control the distribution of rights.

3. The mandated model of Bella-LaPadula

The mandated model of use management is based on confidential document exchange rules adopted by state and government agencies in many countries. The essence of Bella Lapadula's policy is taken from practical life, and a special label called a security level, such as "confidential", "absolutely confidential", etc., is given to those involved in the processing of protected information and documents containing this information. etc. appointment. All levels of security are sorted by priority, for example, the "top secret" level is higher or higher than the "top secret" level. Use control is based on two simple rules, depending on the level of security of the parties involved:

1. An authorized person (subject) has the right to read information only from documents whose level of security is not higher than his level of security.

2. V an authorized person (subject) has the right to include information in documents whose level of security is not lower than his level of security.

The first rule provides protection against the use of information processed by high-level individuals by lower-level individuals. The second rule (a very important rule) eliminates information leakage (knowingly or unknowingly) to high-level participants in the process of processing information.

The Bella and La Padula model. In order to construct the means of restricting the right of use in this model, the concepts of active subjects S 'and passive objects Q are introduced, and the rights of subjects to use passive objects vary. This model is sometimes referred to as the "matrix model that restricts access." Most existing real-time operating systems use the Bella and La Padula models. In this model, the use of an access dispatcher is required, and the protection system is represented by the following trinity:

Z = <S, Q, P>

Here S is the set of subjects, Q is the set of objects, and P is the set of rights to use the objects.

Figure 20.2 Bella-LaPadula model

4. Security role model

The role model is a completely different type of security policy, based on a compromise between the flexibility of managing the use of a discretionary model and the rigidity of the rules governing the use of a mandated model.

In the role model, the concept of "subject" is replaced by the concepts of "user" and "role". A user is a person who works with a system and performs certain service functions. A role is an abstract concept that actively participates in a system and is associated with a limited, logically related set of powers necessary to perform a particular activity.

Role policies are common because they are very close to real life, unlike other rigid and formal policies. In fact, users of the system do not act on behalf of the individual, but perform certain service functions, that is, perform certain roles that are not related to their identity.

When using a role policy, access control is performed in two stages: the first stage specifies a set of powers for each role, including a set of rights to use the object, and the second stage assigns a list of roles to each user. Powers for roles are assigned on the principle of minimum privilege, meaning that each user must have only the minimum set of powers necessary to perform his or her job. The role model describes the system in the form of the following sets (see Figure 20.3):

Figure 20.3. The role model of use management

U - set of users;

R - set of roles;

P - a set of authority to use the object (for example, in the form of a matrix of rights to use);

S is a set of user sessions with the system.

The following relationships are defined for the packages listed above:

$PA \subseteq P \times R$- assigns the powers assigned to each role, and the set of powers is reflected in the set of roles;

Conclusions on security policy models.

Discretionary and mandated security policies are in line with traditional mechanisms adopted in existing automated information systems. For discretionary models, the rights to objects (files) are assigned by the users to whom they belong, and the process authority is determined by the user ID that executes it on behalf of the user. For the mandate model, the level of security of the objects corresponds to the confidentiality of the documents stored in them, and the level of security of the subjects is determined by the category of "permission" of users. Rather, the role policy reflects the applied policy of security. Therefore, there is no clear consistency in this policy. The mechanism for implementing this policy should be developed based on the conditions of the application and the methodology for assigning roles and powers.

RESULTS

The mandated model of use management is based on confidential document exchange rules adopted by state and government agencies in many countries. The essence of Bella Lapadula's policy is taken from practical life, and a special label called a security level, such as "confidential", "absolutely confidential", etc., is given to those involved in the processing of protected information and documents containing this information. etc. appointment. All levels of security are sorted by priority, for example, the "top secret" level is higher or higher than the "top secret" level. Use control is based on two simple rules, depending on the level of security of the parties involved:

1. An authorized person (subject) has the right to read information only from documents whose level of security is not higher than his level of security.

2. V an authorized person (subject) has the right to include information in documents whose level of security is not lower than his level of security.

The first rule provides protection against the use of information processed by high-level individuals by lower-level individuals. The second rule (a very important rule) eliminates information leakage (knowingly or unknowingly) to high-level participants in the process of processing information.

The Bella and La Padula model. In order to construct the means of restricting the right of use in this model, the concepts of active subjects S 'and passive objects Q are introduced, and the rights of subjects to use passive objects vary. This model is sometimes

referred to as the "matrix model that restricts access." Most existing real-time operating systems use the Bella and La Padula models. In this model, the use of an access dispatcher is required, and the protection system is represented by the following trinity:

Z = <S, Q, P>

Here S is the set of subjects, Q is the set of objects, and P is the set of rights to use the objects.

Figure 20.2 Bella-LaPadula model

4. Security role model

The role model is a completely different type of security policy, based on a compromise between the flexibility of managing the use of a discretionary model and the rigidity of the rules governing the use of a mandated model.

In the role model, the concept of "subject" is replaced by the concepts of "user" and "role". A user is a person who works with a system and performs certain service functions. A role is an abstract concept that actively participates in a system and is associated with a limited, logically related set of powers necessary to perform a particular activity.

Role policies are common because they are very close to real life, unlike other rigid and formal policies. In fact, users of the system do not act on behalf of the individual, but perform certain service functions, that is, perform certain roles that are not related to their identity.

DISCUSSION

2. The Harrison-Ruzzo-Ulman discretionary model

As you know, security policy is a general definition of information processing it is understood that a set of procedures and rules, the implementation of which provides protection against a certain set of threats and is a necessary (sometimes sufficient) condition of system security. The formal expression of a security policy is called a security policy model.

Manufacturers of secure information systems use the security model in the following cases:

- development of a formal specification (detailed list) of the developed system security policy;

- in the selection and justification of the basic principles of the architecture of the protected system, which determine the mechanisms of implementation of protection measures;

- in the process of analyzing system security as a reference model;

- confirming the characteristics of the system, which is produced by formal proof of compliance with security policies.

By creating formal security models, consumers will be able to communicate their requirements to manufacturers in a clear and unambiguous manner and assess the suitability of protected systems for their needs.

Qualification experts use the security model as a benchmark when analyzing the adequacy of security policies in protected systems.

The security model is based on the following basic assumptions.

1. A system consists of a set of interacting "subjects" and "objects". Objects can be intuitively thought of as information containers, and subjects can be thought of as executable programs that affect objects in a variety of ways. In such an understanding of the system, the security of information processing is ensured by addressing the issue of subject management of the use of facilities in accordance with the set of rules and restrictions that form the security policy. The system is considered secure if the subjects are not able to violate the rules of the security policy. It should be noted that the definition of "object" and "subject" can vary significantly in different models.

2. All interactions in the system are modeled by establishing certain types of relationships between subjects and objects.

3. All activities are monitored by the interaction monitor and are prohibited or permitted in accordance with the rules of security policy.

4. The security policy is given in the form of rules, according to which all interactions between subjects and objects are obligatory. Interactions that violate these rules are prevented by means of use controls and cannot be carried out.

5. A set of subjects, objects, and the relationships between them (established interactions) determine the "state" of the system. Each system condition is safe or unsafe according to the safety criteria suggested in the model.

6. A key element of the security model is the proof of the theorem that a system in a safe state cannot become dangerous if all the rules and restrictions are followed.

CONCLUSION

The hacker has a clear plan of action and allocates certain resources. His attacks are well thought out and usually take place in several stages. It first collects initial information (type of operating system, services provided, and security measures applied). It then plans an attack based on the information gathered and selects (or even develops) the appropriate tools. He then launches an attack, obtains confidential information, and finally destroys all traces of his actions. Such an attacking professional is usually well-funded and can work alone or on a team of professionals.

An unreliable employee creates the same problem as an industrial spy. On top of that, it is more difficult to determine its existence. It also has to remove the internal protection of the network, which is usually less robust, rather than the external protection of the network. However, in this case, the risk of unauthorized use of corporate information is higher than that of a person with any other malicious intent.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

7 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

8 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

9 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

10 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

11 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

12 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

13 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

14 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

15 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.