THREAT ANALYSIS AND PROTECTIVE MEASURES FOR VOICE-BASED IDENTIFICATION

Yuldasheva Nafisa Salimovna

Tashkent University of Information Technologies named after Muhammad al-Khorazmi, associate professor, Ph.D
E-mail:syuldashevanafisa@gmail.com

KEYWORDS

STRIDE, threat, identification, DOS.

ABSTRACT

This article presents an analysis of the threats and risks that may arise in the implementation of voice-based applications. In particular, the issues of classifying threats according to the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges) methodology, assessing threat risks according to the DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) model, and taking protective measures against them are considered [1,2].

I. Introduction.

In general, voice-based applications can be described as shown in Figure 1. According to it, initially, a command (signal) spoken by the user is entered into the user-side part of the system. This part of the system converts the received voice command into an audio signal and sends it to the server part of the system for processing. Based on the input information, the server generates an appropriate response and returns it to the client or performs an action in the access control system (for example, granting permission). The cloud service can be implemented in this architecture according to the choice and can store information or perform a service.

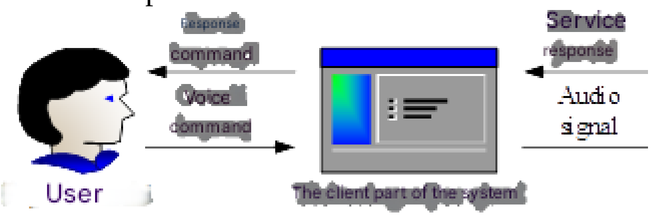

Figure 1. Voice-based application architecture

II. The main part

Threat modeling identifies potential threats to a system and assesses the risk level of the identified threats. This allows you to properly implement security settings for a system before it is deployed. There are several threat modeling tools available, and the STRIDE methodology and tool proposed by Microsoft is widely used in practice.

This methodology allows us to classify threats according to the following factors [3]:

- Attempt to log in to the system using a fake identity – Spoofing;
- Data corruption in the network – Tampering;
- User's failure to acknowledge that an action has been performed – Repudiation;
- Unwanted impact and loss of personal data – Information disclosure;
- Attack on system usability – Denial of Service (DoS);
- Attempt to increase user privilege levels by exploiting vulnerabilities – Elevation of privileges.

DREAD, provided by Microsoft, is mainly used to determine the level of risk posed by threats. In this section, the DREAD model is used to rank and prioritize threats according to their severity level [4]. Using the DREAD model, the severity of a threat can be determined by numerical values (0 (low, difficult), 5 (medium), and 10 (high, easy)) for each of the five categories described below.Table 1 is used to calculate the final rating.

Table 1

Relationship between threat rating and values

Threat rating	Total cost
High	8-10
Middle	4-7
Low	0-3

A description of all 5 factors of the DREAD model is given below [6]:

- *Damage Potential measures the level of damage that can be caused by a threat. This is considered a worst-case scenario if an attacker can exploit the vulnerability to compromise the entire system and data [4].*
- *Reproducibility measures how easily an attack or threat can be replicated.*
- *Exploitability is a measure of how much effort is required to launch an attack. This is considered a worst-case scenario if someone can launch an attack [4].*
- *Affected Users is a measure of how many people would be affected if an attack were launched. It is usually measured as the percentage of users affected.*
- *Discoverability is a measure of how easily a threat can be discovered. If an attack is easily discovered, then the value is 10.*

One of the first steps in threat modeling is to identify existing threats using automated systems. The Microsoft Threat Modeling Tool v.7.3.31026.3 tool was used to perform this task. To do this, it is first necessary to design an expanded form of the system architecture in the software tool, DFD (Data Flow Diagram) view, shown in Figure 1 [6]. In general, the DFD view for voice-based applications is shown in Figure 2 [5]. In this case, the command spoken by the user is initially transmitted as an audio signal to the client part of the system through a microphone. The client part of the application plays an important role, sending information to the server part of the system and, based on the response received from it, to the IoT controller. In addition, the user is notified through a loudspeaker about the attacks that have occurred. In turn, the server part of the application can use cloud services or data storage systems to carry out its activities. The IoT controller can perform a security action (for example, opening a door) by controlling several IoT devices.

Threat Analysis. Based on the above DFD, the following were predetermined for the implementation of the threat analysis for the system:

- It is assumed that there is no physical attack on the data flow within the trust boundary of the device consisting of a microphone, the client part of the voice-based application and the speaker (speaker). In other words, the device is considered trustworthy.
- The analysis is also not performed for the data flow between the IoT controller and IoT devices, and between the server part of the Voice-based application and Cloud services/data storage. The main reason for this is that they are not directly connected to the voice-based device [7].
- In other words, the analysis is performed only for the data flow entering and leaving the voice-based device.

The analysis results obtained using the Microsoft Threat Modeling Tool v.7.3.31026.3 tool [5] are as follows:

1. *The following threats exist for the "**Audio signal" sent from the client part of a voice-based application to the server part of a voice-based application:***

1.1. Spoofing. If an authentication mechanism is not established between the server part of a voice-based application and the client part, a spoofing attack can be carried out. In other words, an unauthorized audio signal can be sent to the server part of a voice-based application by an attacker.

2. *There are the following threats to the **"Voice Command" sent by the user to the Microphone:***

2.1. Spoofing. The voice of a real user can be recorded by an attacker and presented to the system, that is, it can be spoofed.

2.2. Modification. Due to the fact that voice commands are audible to everyone and are difficult to protect, they can easily be recorded, modified and presented by an attacker to obtain unauthorized information from the system or perform a task.

2.3. Denial of service. The microphone transmits the command spoken by the user to the client part of the voice-based system. In this case, there is a possibility of disabling the client part of the system by sending continuous various sound signals to the microphone.

3. *The following threats may exist for the **"Service Response" sent from the server side of a voice-based application to the client side of the application:***

3.1. Modification. If the integrity of the service between the server and client parts of the application is not ensured, it is possible to modify the service request. For example, the attacker can replace the “Reject” response given by the server to the access permission command with “Allow” and, as a result, the IoT controller can allow access.

3.2. Information disclosure. When the confidentiality of the communication between the server and client parts of the system is not ensured, similar to the above case, the attacker can obtain important information. This can then be used by the attacker for malicious purposes.

3.3. Denial of service. Based on the above case, the attacker can launch a DoS attack against the client part of the application. This can be achieved by sending commands or large amounts of data that cause errors in the client side of the application, which are different from the actual data obtained.

3.4. Privilege escalation. By performing a DoS attack or injecting unauthorized data into the client side of the application, an attacker can escalate his privileges. This allows him to have a more serious impact on the system.

4**. The following threats can be implemented against the **"Control Request" data stream sent from the client side of a voice-based application to the IoT controller:

4.1. Spoofing. In the absence of an authentication mechanism between the client part of a system like the one above and the IoT controller, an attacker can send malicious control commands, which can result in unauthorized actions. For example, allowing a door to be opened when it is not authorized.

4.2. Modification. As with the server and client parts of the system, if the integrity of the communication between the client and the IoT controller is not ensured, control requests can be easily modified.

5.** The following threats can be implemented against the **“Motion Response” data stream sent from the IoT controller to the client part of the voice-based application:

5.1. Spoofing. In the absence of an authentication mechanism between the client part of the system and the IoT controller, an attacker can send an arbitrary action response by discrediting the IoT controller.

5.2. Modification. If an integrity mechanism is not implemented between the IoT controller and the client part of the voice-based application, an attacker can send an arbitrary action response.

5.3. Information disclosure. If a confidentiality mechanism is not implemented between the IoT controller and the client part of the voice-based application, an attacker can have full knowledge of the action responses sent.

5.4. Denial of service. If integrity and confidentiality mechanisms are not implemented for this connection, an attacker can disable the client part of the voice-based application by sending a sequence of malicious action responses.

5.5. Privilege escalation. A DoS attack can allow an attacker to escalate their privileges. For example, they can easily do this by capturing the logback information of highly privileged users in the application.

6.** The following threats can be observed for the **"Command Response" sent to the user from the speaker (Speaker):

6.1. Disclosure of information. The disclosure of information to the public through the loudspeaker violates its confidentiality. This could create an opportunity for an attacker to listen to unauthorized information and study the system in depth.

Risk Analysis. The DREAD model was used to calculate the risk level of a total of 16 threats for the 6 data streams mentioned above. Since the DREAD model consists of 5 categories, the overall risk score can be calculated using the expression (D+R+E+A+D)/5 [8]. The risk level analysis of all 16 threats identified above for voice-based systems is presented in Table 2, according to which there are 2 low-risk threats, 10 medium-risk threats, and 4 high-risk threats.

Below are examples of calculating the risk level for some threats. For example, the microphone spoofing threat (1.1) can be used to impersonate a real user or to discredit the voice, thereby gaining the privilege of legitimate users, since there is no authentication mechanism. Therefore, D = 10. Since this threat requires inexpensive equipment to implement, E = 10, and since the attack is easy to implement, R = 10. Since most systems do not pay attention to security issues, and the system does not have the ability to verify the authenticity of the voice, D = 10. Finally, since this type of threat has a serious impact on the user, A = 10. The overall risk level for this threat is 10.v

Table 2

Risk analysis of a voice-based system

Data flow number	Threat number	**D**	**R**	**E**	**A**	**D**	**General**
1	1.1	0	0	10	5	0	3
2	2.1	10	10	10	10	10	**10**
	2.2	10	0	0	10	0	4
	2.3	0	10	0	10	0	4
3	3.1	10	10	10	10	5	**9**
	3.2	10	10	10	10	0	**8**
	3.3	0	10	5	10	10	**7**
	3.4	10	10	0	10	0	6
4	4.1	10	10	5	10	0	**7**
	4.2	10	10	5	10	10	**9**
5	5.1	0	10	5	10	10	**7**
	5.2	0	10	0	10	10	6
	5.3	10	10	5	5	0	6
	5.4	10	10	10	10	10	**10**
	5.5	10	0	0	0	0	2
6	6.1	0	10	10	10	0	6

III. Results

In this article, an analysis of threats to voice-based identification was performed using the STRIDE methodology. The risk level of these threats was assessed using the DREAD model. Protection measures were proposed for threats with a high score. The above protection measures are important in creating voice-based applications and ensuring their security.

List of used literature

1. Hussain S. et al. Threat modelling methodologies: a survey //Sci. Int.(Lahore). – 2014. – T. 26. – №. 4. – C. 1607-1609.
2. Sanfilippo J. et al. Stride-based threat modeling for mysql databases //Proceedings of the Future Technologies Conference (FTC) 2019: Volume 2. – Springer International Publishing, 2020. – C. 368-378.
3. Khan R. et al. STRIDE-based threat modeling for cyber-physical systems //2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). – IEEE, 2017. – C. 1-6.
4. Zhang L. et al. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces //International Journal of Information Security. – 2022. – C. 1-17.
5. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
6. Y. Lei, N. Scheffer, L. Ferrer, M. McLaren, A novel scheme for speaker recognition using a phonetically-aware deep neural network, in: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2014, pp. 1695–1699.
7. Tashev K.A., Fayziyeva D.S., Yuldasheva N.S., Bank tizimlarida zaifliklar va tahdidlar tahlili // "Muhammad al-Xorazmiy avlodlari" ilmiy amaliy va axborot-tahliliy jurnali. № 4 (26), 2023. -B. 218-223
8. Юлдашева Н.С., Холимтаева И.У., Банк тизимида содир этилган фирибгарликни техник усулларининг таҳлили // G.: "Educational Research in Universal Sciences". ISSN: 2181-3515. VOLUME 1 | ISSUE 6 | November, 2022. -P. 158-162