THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE05

PUBLISHED DATE: - 30-05-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue05-05 PAGE NO.: - 37-42

RESEARCH ARTICLE Open Access

A THREAT MODEL FOR VOICE-BASED APPLICATIONS

Nafisa Yuldasheva
Tashkent University Of Information Technologies Named After Muhammad
Al-Khwarizmi Tashkent, Uzbekistan

Abstract

This article provides an analysis of possible threats and risks in the implementation of voice-based applications. In particular, threat classification according to STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges) methodology, threat risk assessment according to DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) model and issues of taking protective measures against them are considered

Keywords Confidentiality; authorization; threat model; integrity; authenticity; STRIDE, DREAD.

INTRODUCTION

In general, voice-based applications can be described as in Figure 1. According to it, initially, the command (signal) given by the user is entered into the client part of the system on the user's side. This subsystem 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, the server generates an appropriate response and can return it to the client or perform an action in the access control system (for example, grant permission). A cloud service can optionally be implemented in this architecture and can store information or perform a service.

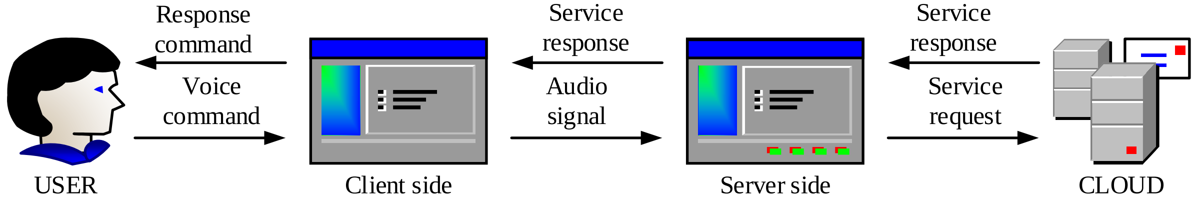

Figure 1. Voice-based application architecture

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

This methodology allows to classify threats according to the following factors [1]:

– attempt to enter the system using a fake ID - spoofing;

– data corruption in the network - tampering;

– failure of the user to admit that he has performed an action - repudiation;

– unwanted influence and loss of privacy of personal data - disclosure of information (Information disclosure);

– attack against system usability - denial of service (DoS);

– the attempt of users to increase the level of privileges by using 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 was used to rank and prioritize threats according to their severity level [2]. 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. Correlation between threat rating and values

Threat rating	Total cost
High	8-10
Medium	4-7
Lower	0-3

The description of all 5 factors of the DREAD model is given below [2]:

– 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 and damage the entire system and data.

– Reproducibility measures how easily an attack or threat can be repeated.

– Exploitability - an indicator that determines how much effort is required to launch an attack. It is considered the worst case if someone can attack.

– The level of affected users (Affected Users) determines how many people will be affected if an attack is launched. It's usually a measure of what percentage of users are affected.

– Threat detection complexity (Discoverability) - an indicator that shows how easily a threat can be detected. If the attack is easily detectable, then the value is 10.

One of the first steps in threat modeling is to identify existing threats using automated systems. Microsoft Threat Modeling Tool v.7.3.31026.3 was used for this task. For this, it is first necessary to design a DFD (Data Flow Diagram) view of the extended form of the system architecture presented in Figure 1 in a software tool [4]. A typical DFD representation for voice-based applications is shown in Figure 2 [3]. In this case, the command spoken by the user is delivered as an audio signal through the microphone to the client part of the system. The client part of the application plays an important role and sends information to the server part of the system and based on the response received from it to the IoT controller. In addition, the user sends a message through the speaker about the insults. In turn, the server side of the application can use cloud services or data storage systems to run its activities. An IoT controller can perform a security action (for example, opening a door) by controlling multiple IoT devices.

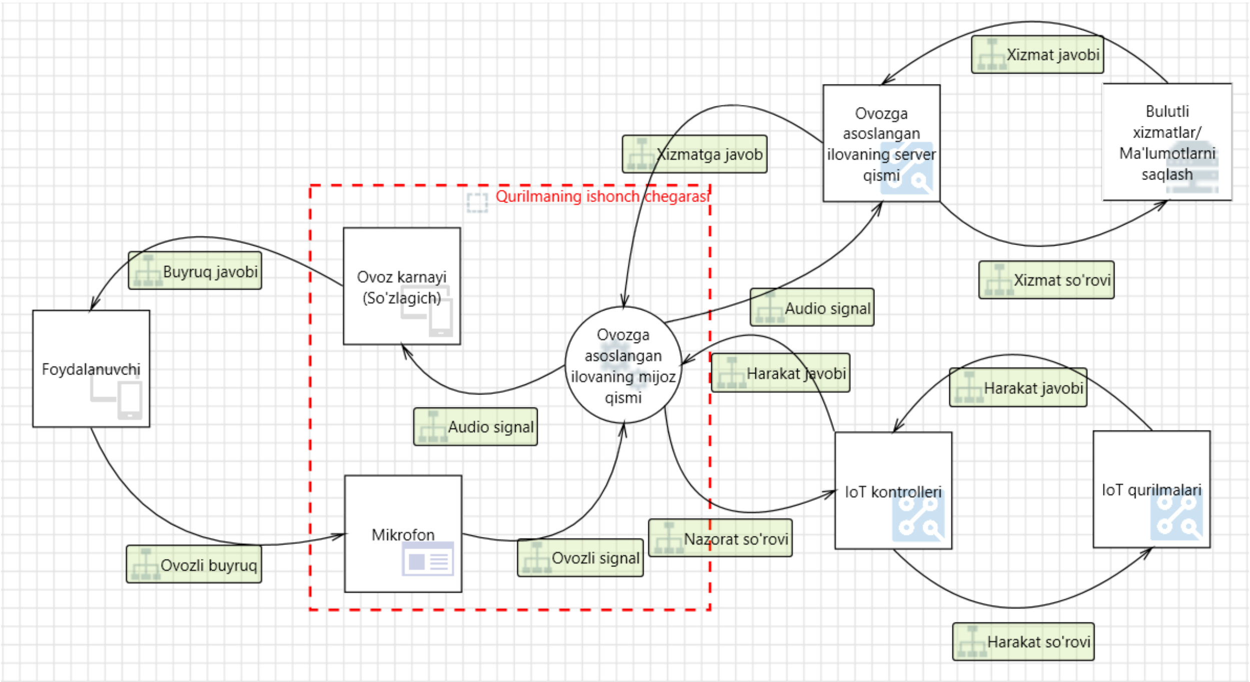

Figure 2. DFD for audio-based applications. A red rectangle represents a voice-based system device.

ANALYSIS OF THREATS.

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

– it is assumed that a physical attack will not take place on the data flow of a device consisting of a microphone, a client part of a voice-based application, and a speaker (speaker). In other words, the device is considered reliable.

– 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 the Cloud services/data storage. The main reason for this is that they are not directly connected to a voice-based device [5].

– In other words, the analysis is performed only for the incoming and outgoing data stream of the voice-based device.

The analysis results obtained using Microsoft Threat Modeling Tool v.7.3.31026.3 [4] are as follows:

1. There are following threats to the "Audio signal" sent from the client part of the voice-based application to the server part of the voice-based application:

1.1. Forgery. If no authentication mechanism is established between the server side and the client side of a voice-based application, a spoofing attack is possible. In other words, an unauthorized audio signal can be sent to the server side of a voice-based application by an attacker.

2. The "Voice command" sent by the user to the microphone has the following threats:

2.1. Forgery. An attacker can record the voice of a real user and submit it to the system, that is, it can be faked.

2.2. Change. Due to the fact that the voice command can be heard by everyone, it is difficult to protect them, it can be easily recorded by an attacker, changed and presented to obtain unauthorized information from the system or perform a task.

2.3. Opt out 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 crashing the client part of the system by continuously sending different sound signals into the microphone.

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

3.1. Change. If service integrity is not ensured between the server and client parts of the application, the service request can be modified. For example, a "Deny" response given by the server to an access permission command can be replaced by an attacker with "Allow", resulting in the IoT controller allowing access.

3.2. Disclosure of information. As in the case above, if the confidentiality of communication between the server and client parts of the system is not ensured, it will be possible for an attacker to obtain important information. This can then be used by an attacker for malicious purposes.

3.3. Opt out of service. Based on the above situation, an attacker will be able to perform a DoS attack against the client part of the application. This can be achieved by sending large amounts of data or commands that cause the client part of the application to fail, which is different from the actual data it receives.

3.4. Increased benefits. By performing a DoS attack or injecting unauthorized data into the client side of the application, an attacker can escalate their privilege. This indicates that it can have a more serious effect on the system.

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

4.1. Forgery. In the absence of an authentication mechanism between the client part of a system similar to the above and the IoT controller, an attacker can send malicious control commands and, as a result, perform unauthorized actions. For example, to be allowed to open the door even when it is not allowed.

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

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

5.1. Forgery. 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 an arbitrary action response by discrediting the IoT controller.

5.2. Change. If no integrity mechanism is implemented between the IoT controller and the client side of the voice-based application, it is possible for an attacker to send an arbitrary action response.

5.3. Disclosure of information. If no confidentiality mechanism is implemented between the IoT controller and the client side of the voice-based application, an attacker may have complete knowledge of the action responses that are sent.

5.4. Opt out of service. If integrity and confidentiality mechanisms are not implemented for this connection, an attacker could crash the client side of a voice-based application by sending a sequence of malicious action responses.

5.5. Increased benefits. As a result of a DoS attack, an attacker can increase his privilege. For example, an application can easily do this by capturing the log data of high-privileged users.

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

6.1. Disclosure of information. As a result of public disclosure of information through the loudspeaker, their confidentiality is violated. This will allow an attacker to eavesdrop on unauthorized information and explore 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 listed above. Since the DREAD model consists of 5 categories, the total risk result can be calculated using the expression (D+R+E+A+D)/5 [6].

An analysis of the risk level of all 16 threats identified above for voice-based systems is presented in Table 2, according to which there are 2 threats with a low risk level, 10 with a medium risk level and 4 with a high risk level.

Table 2. Risk analysis of a voice-based system

Data flow number	Threat number	D	R	E	A	D	Total
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

Below are examples of how to calculate the risk level for some threats. For example, a microphone spoofing threat (1.1) may privilege legitimate users due to the possibility of impersonating a genuine user or discrediting a voice when there is no authentication mechanism in place. Therefore, D = 10. Since this threat requires inexpensive equipment, E = 10, R = 10 due to the ease of attack. In most systems, D = 10 due to the lack of security concerns, and the inability of the system to determine the authenticity of the voice. Finally, A = 10 because this type of threat has a serious impact on the user. The overall risk level for this threat is 10.

The protective measures required to prevent the above mentioned threats are presented in Table 3 [5].

Table 3. Defense measures against identified threats

Data flow number	Threat number	Countermeasures
1	**2**	**3**
1	1.1	Forgery can be prevented by implementing authentication mechanisms.
2	2.1	Validation of the voice command is required, for example, using a voice "aliveness" mechanism.
	2.2	Using mechanisms to distinguish between modified and real voice commands.
	2.3	Reducing the frequency of audio by filtering frequencies above the audio frequency.
3	3.1	To ensure the authenticity of service responses, it is required to use cryptographic mechanisms or use secure communication channels.

1	2	3
	3.2	Use of secure communication channels, or cryptographic protection of messages.
	3.3	Limiting the number of service responses, or filtering received commands and responses.
	3.4	It is necessary to use mechanisms for checking the length and validity of the message.
4	4.1	Identifying the intruder using authentication mechanisms.
	4.2	Use of cryptographic mechanisms to ensure the integrity of control requests.
5	5.1	Identifying the intruder using authentication mechanisms.
	5.2	Using cryptographic mechanisms to ensure the integrity of action responses.
	5.3	Use of secure communication channels, or cryptographic protection of action responses.
	5.4	Use mechanisms to limit the number of action responses or filter them.
	5.5	It is necessary to use mechanisms for checking the length and validity of the incoming message.
6	6.1	Ensure that response commands do not disclose sensitive information about the user.

The safeguards listed above are critical to building and securing voice-based applications.

REFERANCE

1. 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. – С. 1-6.
2. 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. – С. 1-17.
3. Suprihanto D., Wardoyo R., Mustofa K. Determination of weighting assessment on DREAD model using profile matching //International Journal of Advanced Computer Science and Applications. – 2018. – Т. 9. – №. 10. – С. 68-72.
4. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
5. 5. 76. 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
6. 6. 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