Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 6444-6451

Threat modeling and classification for e-learning systems using STRIDE technique

Rawabi Nazal Alhamad [a], Mashael Mohammed Aldhali [b], Saloua Hendaoui [c]

a College of Computer and Information Science, Cybersecurity Department, Jouf University, 421204015@ju.edu.sa

b College of Computer and Information Science, Cybersecurity Department, Jouf University, 421205963@ju.edu.sa

c College of Computer and Information Science, Cybersecurity Department, Jouf University, selhechi@ju.edu.sa

Abstract: In this study, the most driving and mature Threat Modeling strategy STRIDE, that has been proposed by Microsoft, is utilized to recognize all potential dangers to E-learning frameworks. Security dangers to an e-learning framework are investigated and talked about. Besides, a rundown of countermeasures is recommended to all the more likely plan and execute framework security arrangements against e-learning insider and untouchable dangers.

Keywords: *E-learning, Threat, STRID*

1. Introduction

Dangers can have destroying results. Assaults can debilitate frameworks totally or lead to the spilling of touchy data, which would lessen buyer trust in the framework supplier. Fixing programming security issues right off the bat in the improvement life-cycle decreases its expense significantly. To keep dangers from exploiting framework imperfections, directors can utilize more than one string model to assess hazards and focus on alleviation.

Nowadays with the dramatic expansion of cloud-based E-learning technologies which make almost every student is dealing with a system or another. And that may lead this industry to face a variety of threats. The number of threats grows and differs as technology changes and expand. For example, due to the covid 19 epidemic and the un-predictable reliance on e-learning platforms where wide different systems and technologies are increasingly integrated into a wide range of educational institutes along with its numerous physical devices that leave users' data vulnerable to extraction through a series of device vulnerabilities.

Generally, thread models are used to create:

- An deliberation of the framework.
- Profiles of possible assailants, including their objectives and strategies.
- A list of potential dangers that might emerge

Each system can create its thread model or can use one of the known ready-made thread modeling software. In this paper, we will be offering a general implementation of STRIDE model for a cloud-based E-Learning System. We had applied this paper through the contribution of one of the e-learning provider companies in the region **(Classera).**

2. STRIDE MODEL

STRIDE is considered one of the leading and most mature Danger Modeling systems in the product business. The achievement of this technique is a result of a very much organized way to deal with Threat Modeling, and incredible help and assets for clients. Step applies an overall arrangement of realized dangers dependent on its name, which is a memory helper (Spoofing, Tampering of information, Repudiation, Information Disclosure, Denial of administration, Elevation of advantage). Table 1 is showing the STRID model definition.

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Table 1. STRIDE model description

STRIDE model process goes through 5 main phases:

1- Identifying assets and access points: Assets is any physical or logical that have a business value and should be protected against misuse or attacks, as Login credentials, encryption keys, user details, credit card details, system devices,...etc, while access points are where certain security measures should be taken to protect data while it enters or exits from the system.

2-Defining the Trust levels of framework clients: Trust levels address the entrance rights allowed to elements (human clients, gadgets, and administrations).

3-DFD (information stream outline): DFD is a significant level method of dismantling the framework and zeroing in on its utilitarian parts and investigating the progressions of information through the framework parts [6].

DFD assists with recognizing dangers and to distinguish which resources they connect with. Figure3. shows the DFD for the e-framework,

4-Identify and arrange Threats: Table 2 sums up the recognized dangers, which are arranged by the accompanying sorts:

validation, approval and access, security, just as evaluating and logging dangers.

5- Mitigation Plan: Table 3 illustrates the countermeasures for the identified threats mapped to each of the STRIDE components.

3. STRIDE model implementation for e-learning systems

In this section, we illustrate the process of implementing the STRIDE model for e-learning systems. E-learning comprises the use of information and communication technologies (ICT) to offer different, user-group-specific learning services to participants (Students, Instructors, Admins, etc.) who are in different locations.

The E-learning system structure is consisting 3 main domains:

- Users Portal /Interface
- The System Infrastructure
- The physical & Logical Sources.

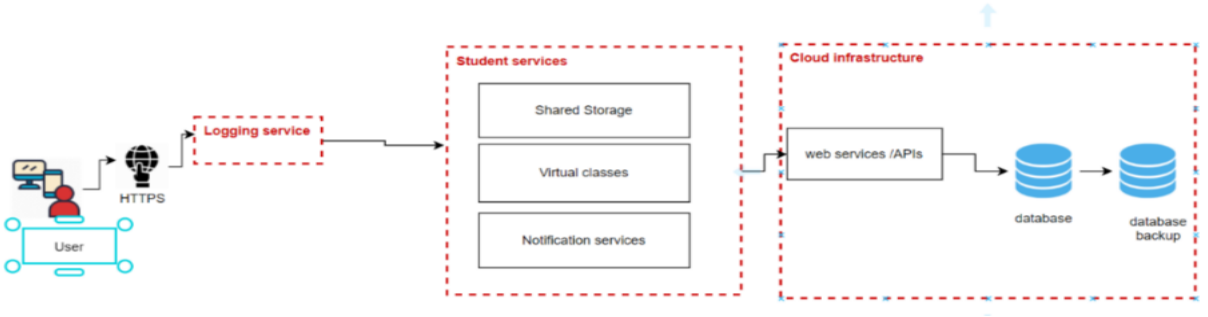

Figure.1 illustrates the main components and users related to each domain.

Figure.1 Architecture overview of the E-Learning system.

The threat modeling phases are:

1- Assets were defined and classified per domain as follows:

D1. Users Portal	**D2. infrastructure**	**D3. sources**
-Users credentials -User's communication devices -Users' data -Educational Content	-SIS servers Services Servers -Digital Libraries	-User Credentials -Terminal devices (Pcs, laptops, tablets , smartphones ,..) -Users related data retrieved through terminals

Table 2: Asset's classification

2- Defining the entities and trust levels:

Trust levels address the entrance rights conceded to elements (clients, gadgets, and administrations) as displayed in Figure 2., and upheld by the framework. For the most part, dangers can begin from two essential sources: inward specialists (somebody with approved admittance) or potentially outside specialists (somebody with unapproved access) [1]. This review will zero in on the insiders just as it has been concurred by many well-informed authorities that insiders have a higher impact than untouchables. Insiders are completely or somewhat believed subjects with authentic access keys to assets**.**

According to a recent report, 58% of all security incidents can be attributed to insiders [2].

Figure 2. shows the cloud-based e-learning system entities & trust levels from the provider.

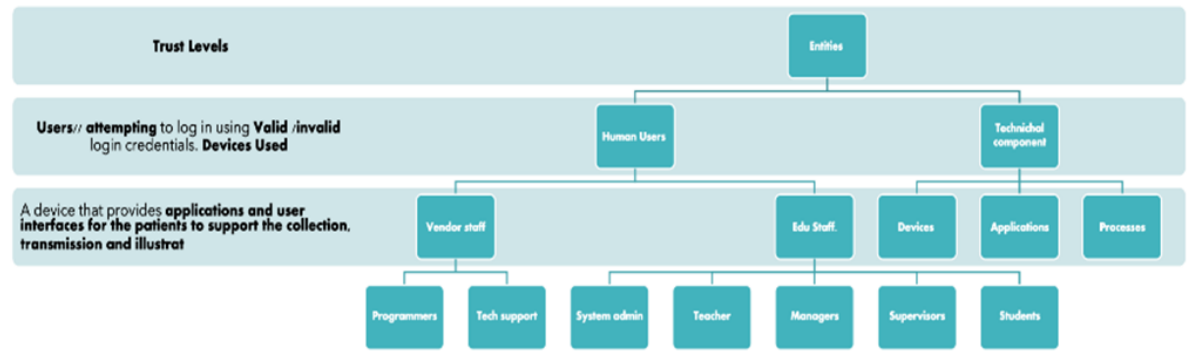

Figure 2: Entities of E-learning system.

Entities of the e-learning system, as shown in figure 2, are:

(a) - Vendor Staff: are all technical team members who have access to the full system backend & frontend.

(b) - System administrator: is responsible for system setup, operation & managing the first level maintenance. The system administrator has access to all system interfaces & Users credentials.

(c) - Other users: each has his own access to his role portal /app only with the privileges granted to them and their personal information and contents.

4.E-learning DFD

As mentioned in section 1, the e-learning data flow diagram represents the data flow and between system entities and trust.

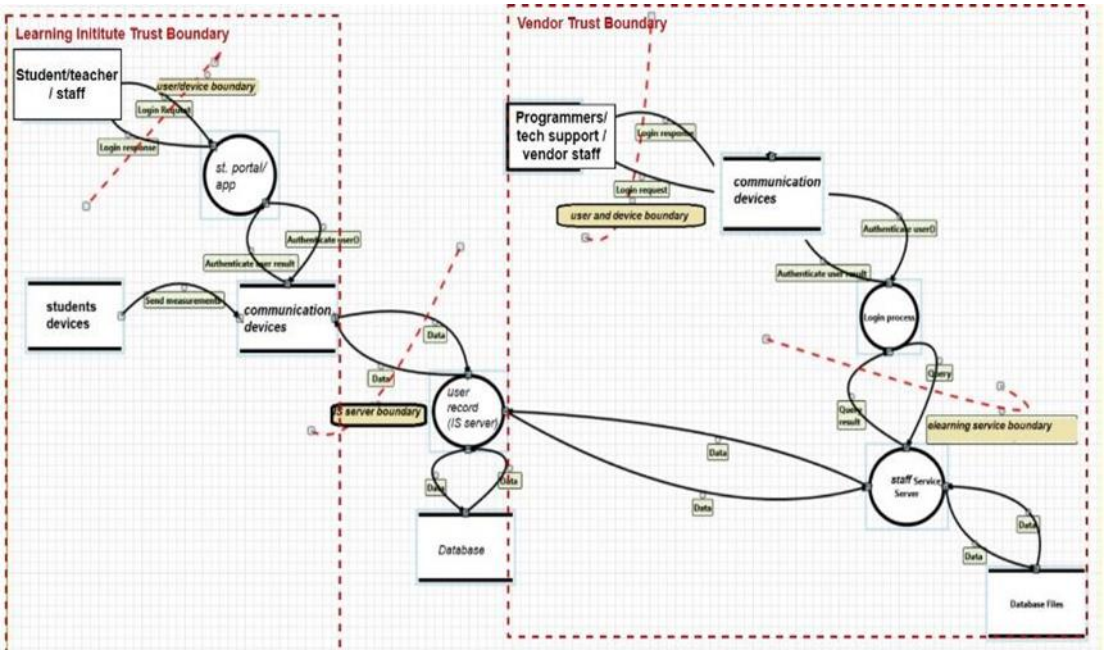

Figure 3: E-learning threat model DFD

5.Identifying and classifying threats

According to the entities & data flow diagram that had been defined, threats were defined and classified into 4 main categories:

- Threat Class 1 (T1): Authentication Threats: unapproved use or abuse of approved client personalities and login accreditations.
- Threat Class 2 (T2): Authorization and Access Threats: unapproved access (counting perusing, compose, change, erase) to private information.
- Threat Class 3 (T3): Privacy Threats: unapproved exposure to delicate information.
- Threat Class 4 (T4): Auditing and Logging Threats: dubious exercises recognized, for example, foot printing or conceivable secret key, breaking endeavors before double-dealing happens.

We summarize in table e 2 the possible threats.

Threat No	**AT: Authentication Threats**		
	Description	**STRIDE**	**Impact**
AT .1	Vendor credentials loss or sharing	S	High
AT.2	End User credentials loss or sharing	S	Low
AT.3	Identity theft and isuse	E	High

AT.4	End User Identity spoofing	S	Low
AT.5	Spoofing of Vendor source /device	S	High
AT.6	Spoofing of End User source/device	S	Medium

Threat No	**AAT: Authorization and Access Threats**		
	Description	**STRIDE**	**Impact**
AAT .1	Vendor Stolen credentials that cause Unauthorized access to system code/data	E	High
AAT.2	End User Stolen credentials that cause Unauthorized access to user portal	E	Low
AAT.3	Unauthorized access as system admin	E	High
AAT.4	Data tampering: Programmer or technical support team accidentally modified or deleted data	T	High
AAT.5	Data tampering: System admin or teacher accidentally modified or deleted data	T	Medium
AAT.6	Unauthorized access to administration interfaces: malicious users may be able to gain access to configuration management through administration interfaces.	E	High

Threat No	**PT: Privacy Threats**		
	Description	**STRIDE**	**Impact**
PT .1	Unauthorized disclosure: system admins or vendor insider team accessed unauthorized confidential data using malware or file sharing tool installed on their devices	I	High
PT.2	Unauthorized disclosure: End User accessed unauthorized confidential data using malware or file sharing tool installed on their communication server.	I	Medium
PT.3	Lost/ stolen device : End user lost or stolen devices that would cause exposure to credentials and personal data	I	High

Threat No	**ALT: Auditing and Logging Threats**		
	Description	**STRIDE**	**Impact**
ALT .1	Potential data repudiation: System admins or users deny or claim not receiving, writing or editing data	R	High
ALT.2	Log files tampering: system admins or users could delete or update log files in any way.	T	High
ALT.3	Insufficient logging: not correct or enough logging data to handle repudiation claims.	I	High

Table 2. The possible threats.

6. Mitigation and counterneasures

As potential threats are clearly defined and analyzed, it's time to plan the needed mitigation and countermeasures corresponding to each STRIDE. We illustrate in table 3 the possible countermeasures.

STRIDE	Threats	Countermeasures
Spoofing	AT.1 , AT.2, AT.4, AT.5, AT.6	- Strong authentication - Encryption - Cryptographic protocols
Tampering	AAT.5 , AAT.6 , PT.3	- Strong authorization - Data hashing and signing - Secure communication links
Repudiation	T4.1	- Secure audit trails
Information disclosure	PT.1 , PT.2 , PT.3 , ALT.3	- Strong authorization - Encryption - Secure communication links
Elevation of privilege	AT.3 , AAT.1 , AAT.2 , AAT.3 , AAT.6	- Principle of least privilege

Table 3. Mitigation and Countermeasures

8.Conclusion

The thought behind making a danger model for e-learning frameworks is to assist with improving framework security as far as ensuring the local area data (understudies, guardians, educators, instructive staff, …) from security dangers, like patient information exposure and additionally unapproved access or adjustment by assailants, among others. In this work, a danger. The model cycle for e-learning frameworks utilizing Microsoft danger displaying apparatus STRIDE that was set up in 2014.

To get ready for danger relief, framework resources, danger specialists, unfriendly activities, dangers, and their belongings just as a rundown of countermeasures were distinguished and examined. This work will be utilized to foster security necessities and to more readily plan and carry out framework assurance arrangements against e-learning application dangers.

References

1. M. Gerdes, Geir M. Køien, M. Abomhara, "A STRIDE-Based Threat Model for Telehealth Systems" University of Agder, Norway, Nov 2015.
2. Michael McGrath, Threat Modelling for Legacy Enterprise Applications, Submitted to the Higher Education and Training Awards Council (HETAC), August 2013.
3. Nataliya Shevchenko, Threat Modeling: 12 Available Methods Software Engineering Institute, Dec 2018.

4. S. F. Burns, “Threat modeling: A process to ensure application security,” GIAC Security Essentials Certification (GSEC) Practical Assignment, 2005.
5. S. Myagmar, A. J. Lee, and W. Yurcik, “Threat modeling as a basis for security requirements,” in Symposium on requirements engineering for information security (SREIS), vol. 2005.
6. SPENCER COURSEN, Data Insider Journal at : https://digitalguardian.com/blog/insider-outsider-data-security-threats