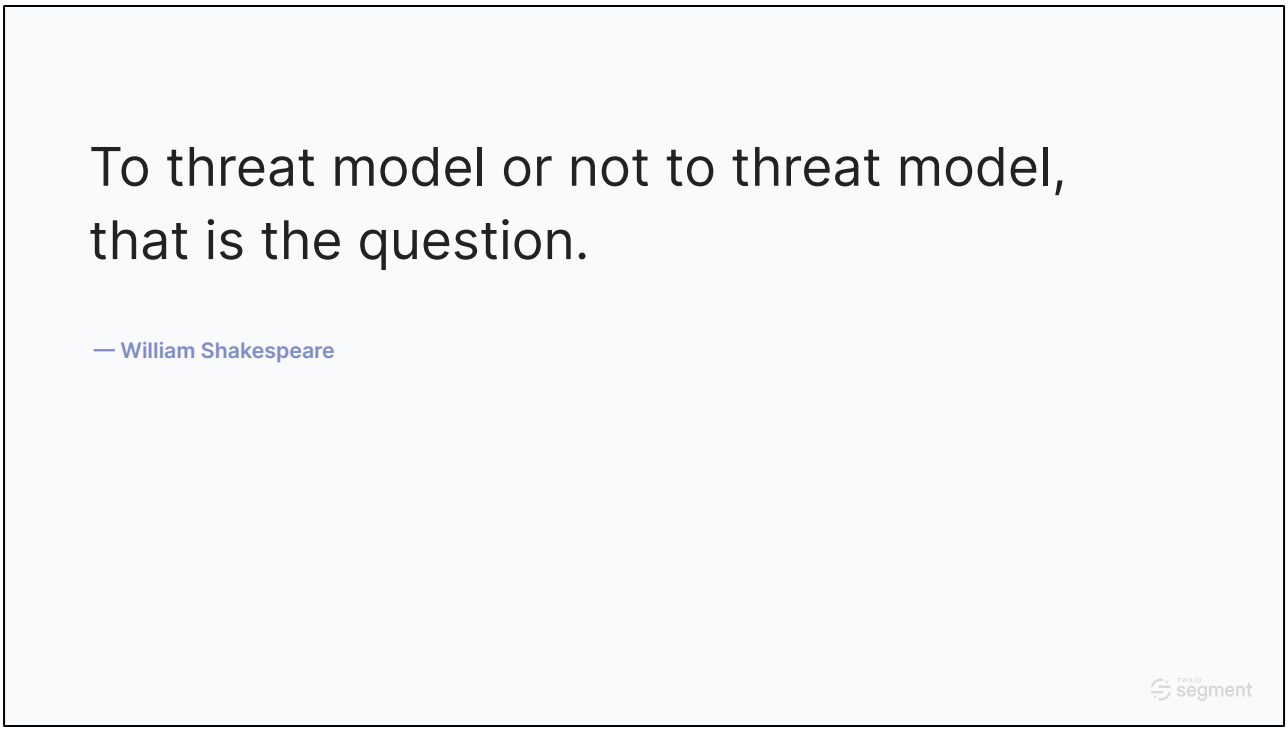
TWILIO segment

Live Threat Modeling

3



Clearly Shakespeare didn’t take this training, otherwise he would have suggested to threat model

Agenda

- Review Threat Modeling
- Feature Context
- Live Threat Model
- Next steps

Agenda is pretty straightforward

- Will review STRIDE and finding threats
- We will review the feature we are going to threat model
- We will then perform an actual threat model on a system
- Talk about where Engineering is going from here, what are expectations

Goals

- Perform an actual Threat Modeling
- ~~Become a Threat Modeling legend~~

This isn’t training in the same vein as we did in the past, everyone will need to understand the feature and everyone will need to help perform the threat model.

Review

Review — Threat Model Steps

- Breaking down the feature
- Find threats
- Prioritize threats
- Mitigate threats

We break down Threat Modeling into four phases:

- Break down the feature - basically this is our Software Defined Document (SDD), written documentation on what the system is, there are diagrams in there, all of the details we need to discover threats
- Find threats - in this phase, we review the documentation and work as a team to discover the different threats to the system
- Prioritize threats - As a team, we will review the threats and prioritize them
- Mitigate threats - Finally we figure out which of the threats we are going to address and go ahead to address them

Diversity

Why is diversity important to Threat Modeling?

- Threat Modeling is a team sport
- Different life experience helps
- Different career experience helps
- Different educational background helps

Threat modeling is a team sport and the more diverse your team members, the better outcome you will have. Everyone has different life experiences, career paths and knowledge, which is a good thing.

I live in my bubble and it is hard for me to think “outside the box”. I am a collection of my experiences and I will rely on that when threat modeling, combining all of our experiences will help build a more robust threat model. **Feel free to DM folks if they are quiet when we go through the actual threat model**, we need everyone’s participation today.

Empathy

Why is empathy important to Threat Modeling?

- Feature built by a real person
- No blaming or shaming
- Let's teach each other to become better

We are humans, but we need to remember that other humans built the tool

Threat Modeling should be very similar to retrospective meetings

- There is no blaming and no shaming
- Threat modeling is to improve our security posture and finding how to become better
- Diversity is important because we all look at the problem differently
- Empathy is important because our coworkers have built this feature
- This is a place to learn and build something even better

Threat modeling is a team sport, we help each other to win.

Review — STRIDE

S Spoofing

T Tampering

R Repudiation

I Information Disclosure

D Denial of Service

E Elevation of Privilege

If you recall, we use STRIDE to help find threats in the system, I am going to quickly run through the example that we used last time to refresh your memory.

STRIDE Example: Segment Surveys

I hope that you remember this from the last threat modeling session

Segment Surveys

In order to better understand our clients, Segment has created a Survey Tool to help gather data and understand how the clients think about our application.

The tool itself is very simple, there is a web application that shows the survey question to the anonymous users and collects their answers.

There is a separate web application that shows the results of the survey to Segment's Admin users.

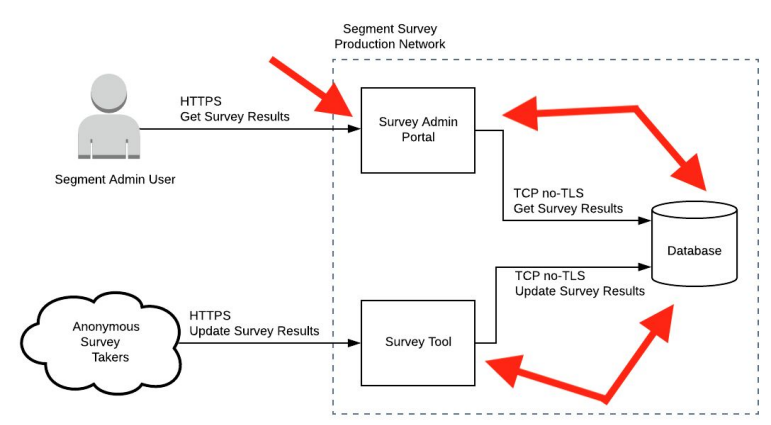
The entire system is in a separate account in our Production network. No other service has access to this system.

Where should we look to find threats?

READ THE SLIDE

Segment Surveys — Spoofing

Spoofing: A situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.



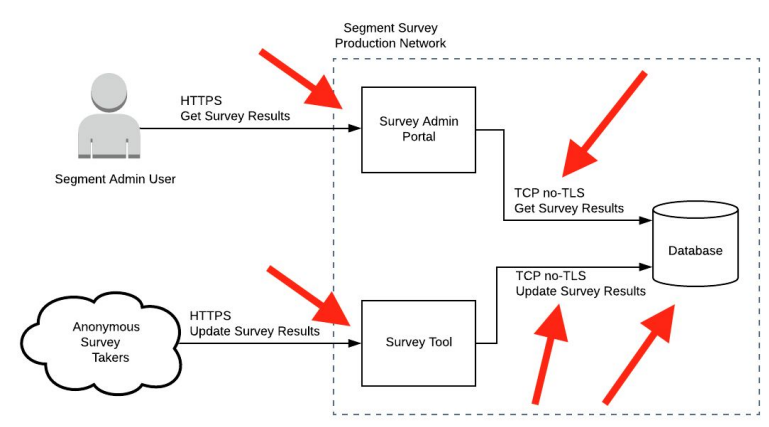
I am going to read out the type of vulnerabilities that can be discovered

Spoofing

- What is happening between the Survey Tool and the database, how is authentication happening?
- Similar question for between Survey Admin Portal and Database
- What about Segment Admin User, how are they authenticating?

Segment Surveys — Tampering

Tampering: Interfere with something in order to cause damage or make unauthorized alterations.

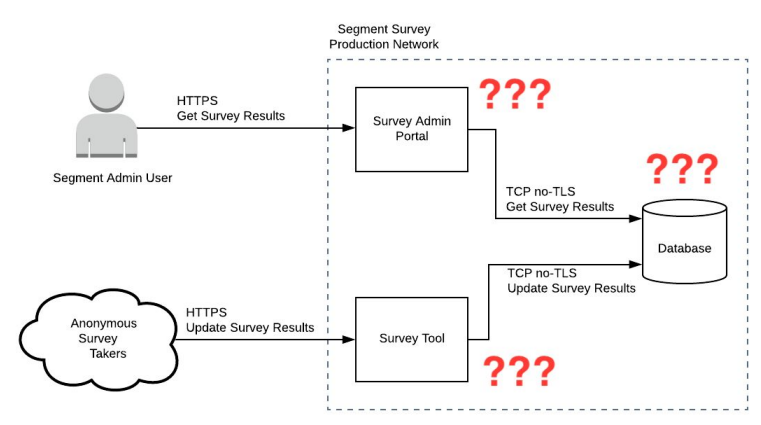


Tampering

- Is there any client side controls in the survey?
    - Perhaps a max character limit or if it is a multiple select, would you only be able to select 3 max checkboxes? Can we bypass those controls by hitting Survey Tool directly?
- Similar to the Admin Portal, is there a way for the admin to bypass any client side controls that we have put in place or tamper with the request itself?
- There is no-TLS to connect to the database, is there a way for someone to gain access to the production network and tamper with the non-TLS requests?
- Is there a way for anyone to gain access to the database? Potential insider attack can be someone modify the results of the survey to something they like?

Segment Surveys — Repudiation

Repudiation: The ability of denying that an action or an event has occurred.

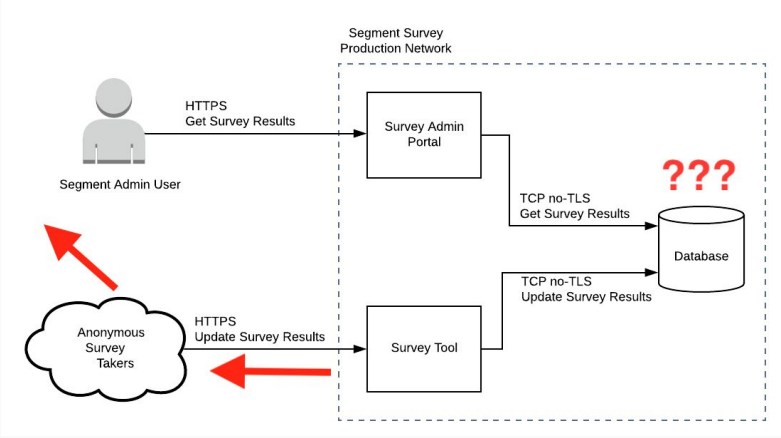


Repudiation

- What information are we logging?
- Where are we logging the information?
- Do we log access to the Survey Results application?
- Do we log login Segment Admin login requests?
- So many questions around logging

Segment Surveys — Information Disclosure

Information Disclosure: Exposing information to someone not authorized to see it.

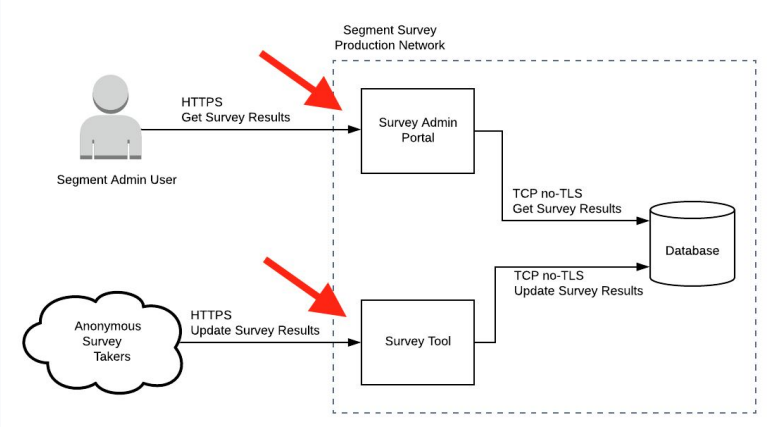


Information Disclosure

- Are we accidentally sending too much information back to the anonymous survey takers? Error information? Response headers?
- Can someone post the anonymous link on the internet, what implications would that have? Do we need to protect the questions themselves? Are the questions sensitive?
- Is it possible to confirm that the database cannot be accessed by anything other than the Survey Admin Portal and Survey Tool, are there other services on the Production Network?
- Is there sensitive information in the database (PHI for example), how is that information protected, can a DBA see that information?
- If we are storing admin user credentials, how are they stored in the database?

Segment Surveys — Denial of Service

Denial of Service: Deny or degrade service to users.

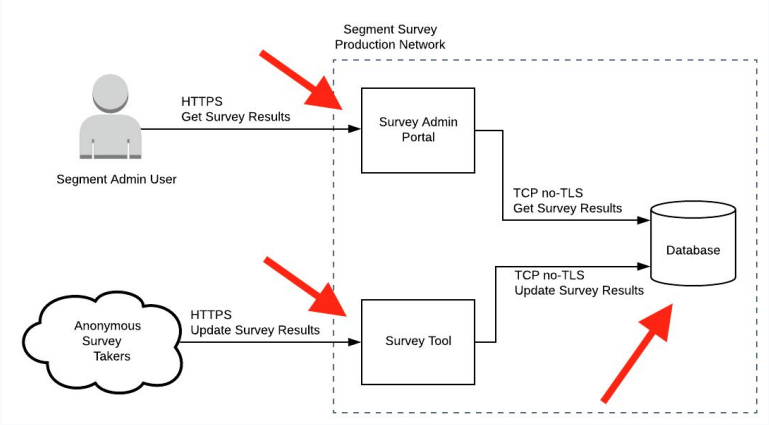


Denial of Service

- How do you prevent an anonymous user accessing the survey 1M times and degrading performance for the admins reviewing the results?
- Is there a way to perform an application dos? If there is an admin, can they get the results of many surveys at once or a survey over a long period of time?
- Can a respondent hold the HTTP connection open?
- Can a respondent submit gigabytes of information for an open-ended question?

Segment Surveys — Elevation of Privilege

Elevation of Privilege: Elevation of Privilege refers to gaining access that one should not have.

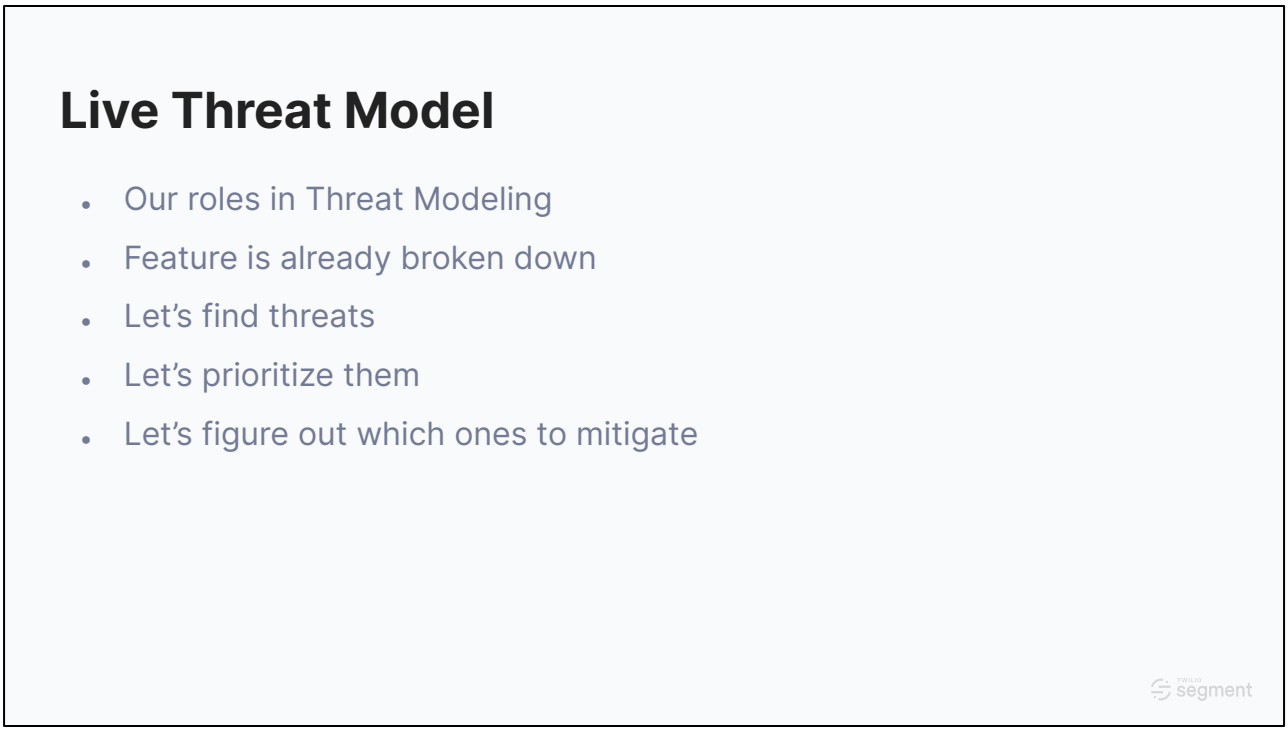


Elevation of Privilege

- How do we give access to the survey to anonymous users?
- Is there a way for anonymous users to access the Survey Admin Portal?
- Are there multiple roles for the Survey Admin Portal?
- Are we implementing least privilege for the role accessing the database?
- If there were to be a SQL injection vulnerability, would it be possible for the malicious actor to delete the database?

Live Threat Model

segment



Live Threat Model

Action: send link of the Threat Modeling document to the channel

I will facilitate the conversation, but everyone will need to be involved.

Notes

- Since there are several folks in this group and there may be several people talking at once, if you have a thought, please write it down and then bring it up to the group, that way you won’t lose your thought
- Your goal is to review the system and try to find ways that will abuse it, everyone’s job to find threats, everyone needs to contribute
- We will prioritize the vulnerabilities towards the end of the exercise and we will decide which ones need to be addressed in the short, medium and long terms

Feature Context

segment

Feature Context

Member of the team will describe their feature/system in detail.

Goals

- Understand the feature's purpose and how it works
- Figure out the assets of the system
- Write notes about any security concerns that you may have
- Think about ways to make the feature not work as intended

Go to the document and have an engineer explain the feature and then move through the document and start to threat model the system

Phew,
almost done!

Goals

- DONE - Perform an actual Threat Modeling
- DONE - Became a Threat Modeling legend

Goals

- You have completed the threat modeling exercise on a live system
- You all did great and are all legends!

Next Steps

- You are in the driver's seat now!
- You lead, Security supports
  - Engineering to run Threat Modeling sessions
  - Security sits in and helps when necessary
- All new SDDs should have
  - Feature breakdown
  - List of prioritized threats
  - Tickets for threats to mitigate
  - Comments for threats that are accepted

Read the slide


TWILIO
segment
You can Threat Model!