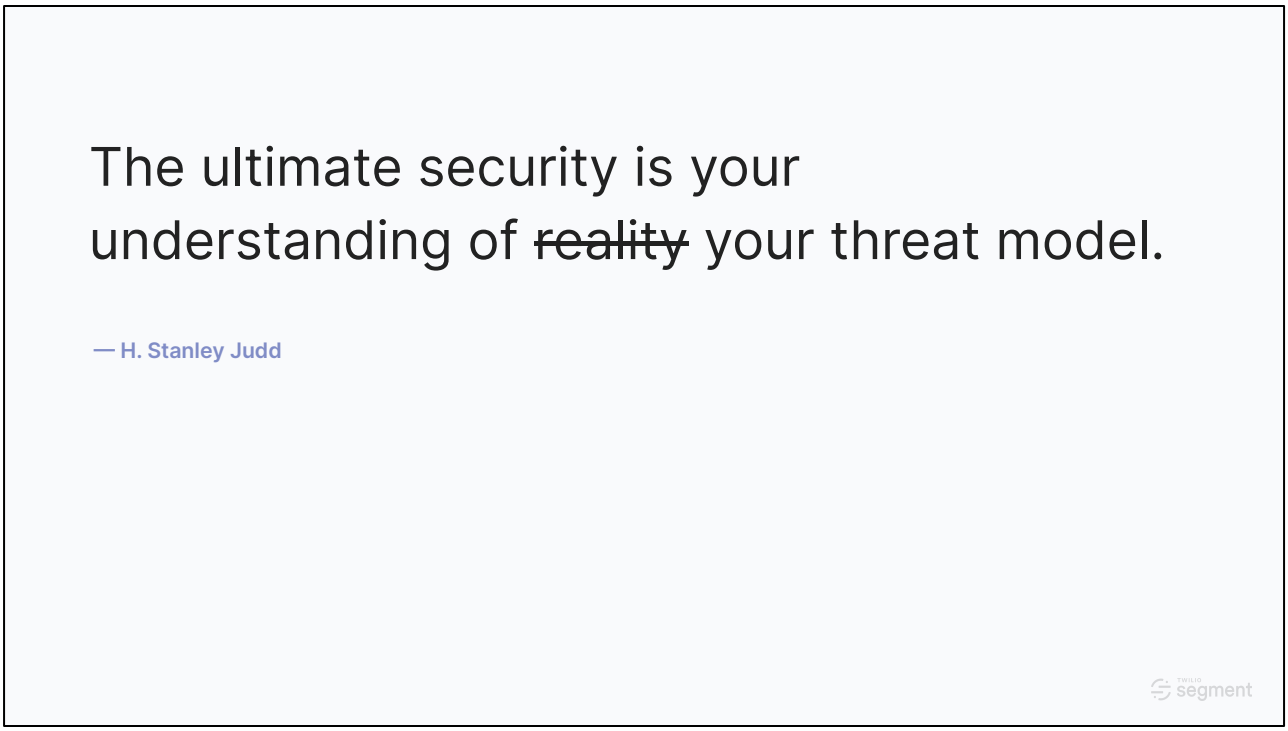
TWILIO segment

Foundations of Threat Modeling

Updated March 2021

2



Always great to start off with a butchered quote.

Agenda

- Assets
- Diversity
- Review
- Examples
- Next steps

Agenda is pretty straightforward

- We are going to go over a few new items for theory (asset, diversity)
- We will review what we covered last training
- Then jump into some hands on examples to get more threat modeling practice

Goals

- Become more familiar with Threat Modeling
- Get our hands dirty with exercises
- Be comfortable asking security questions

What are the goals for this training?

Goals:

- We know how to threat model, but we hope to get better at it
- Focus most of our efforts on hands on exercises
- Really get comfortable reading documents and asking security questions

Quick reminder, we are not trying to make you a threat modeling legend, that will come over time.

Assets

Definition: any item within your threat model that you want to protect.

- TV vs empty pop cans
- Do we care about all data?
- What data should we care about?

When threat modeling, it is important to understand what you are trying to protect in your system or feature. For threat modeling purposes, you can classify an asset as anything you think is worth protecting.

Let's think about the home protection example from the previous threat modeling session. In particular, let's think about protecting your TV vs protecting empty bottles. Technically they both have value, but one has more value than the other and it makes more sense to protect it more than the other.

Now, let's think about those assets with respect to data that we have in our system. Please note that you can think of an asset as other items as well (infrastructure, systems, reputation, etc), but we want to focus on data.

There are different ways to classify data. At Segment we classify them in four categories:

- Public - data that is available on our marketing website and for consumption of the general public - our application's features, press releases, whitepapers, etc
- Confidential - data that is not available for public consumption and should be for Segment eyes only - Software architectural diagrams, our emails, production data that belongs to Segment, etc
- Restricted - data that can only be accessed if absolutely required - Customer data, Customer PII, etc
- Secret - the most sensitive of data, items that only the application

- should have access to - Customer API keys, Encryption keys, Passwords

When threat modeling, we need to identify the assets and the type of data that is being processed or stored in the system. Although it is important to protect public data, we should spend more time and effort protecting secret data.

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 our exercises.

If we go back to the housing example from the first workshop, we talked about a thief being the main concern and we only had a budget of $1000 for protecting the home. **How much would you spend to protect your home and what are you most concerned with?**

The point isn’t about home security, but the fact that everyone has a different opinion about the different threats that they see. It is awesome to have a bunch of different people together when you threat model, the more varied the experience, the better threats/risks you will get out.

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

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, we are going to review these vulnerability classes once more, but with a new exercise.

STRIDE Example: Segment Surveys

We are going to go through a couple of exercises to get better at finding risks to a system.

The first exercise is a warm up, let’s stretch our threat modeling limbs and we will do this with the entire group.

The second one we will review a short design document and come up with our threats and we will breakout into smaller groups.

Ok, let’s talk about a FAKE feature Segment Surveys!

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.

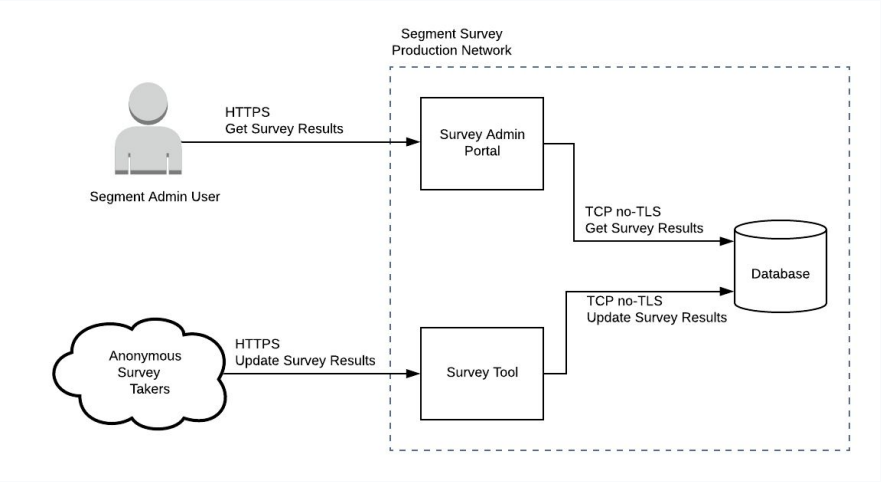
Where should we look to find threats?

TWILIO segment

READ THE SLIDE

Remind the team that this is a warm up exercise and that we will be doing it together.

Segment Surveys — Architecture



segment

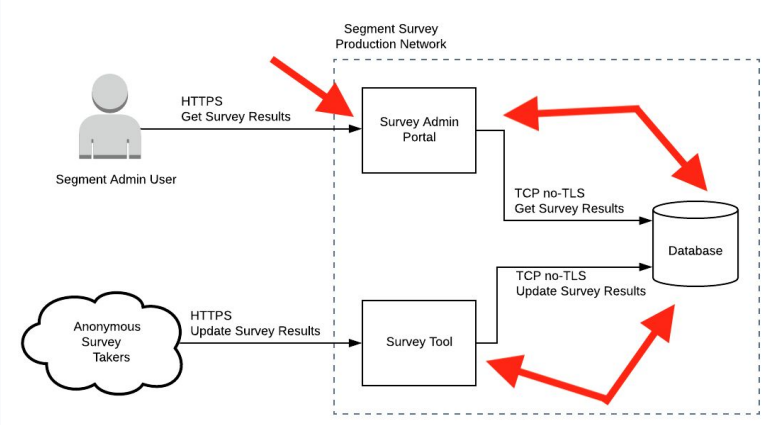
Talk about the architecture of this particular diagram

- It is a very simple system
- Data comes in from the anonymous survey takers and it gets stored into the database
- Admin users are able to generate reports from the data collected from the surveys, which they access from the survey admin portal
- Everything lives in a production network

This system is purposefully vague because I want to make sure that we have questions.

Segment Surveys — Spoofing

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



segment

What are these red arrows? They have been added think about places that we can ask about the defensive controls or the possibility of vulnerabilities.

Since we are talking about spoofing, which is related to authentication. We want to know:

- 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?

The point of this exercise is to ask the right question or question the defensive controls that may or may not be in place.

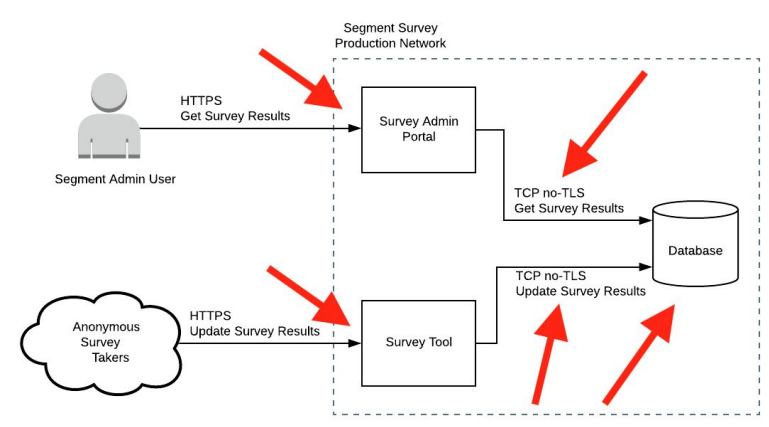
The red arrows are to help you, but you might even want to go deeper than the red arrows

- You may have questions about anonymous users, how do we ensure that each submission of survey results is separate, but still anonymous?
- Or, you might have a question about access to the database itself, how on the team can access it and how do they authenticate?
- Does the Segment Admin users have access to MFA?

The above questions are valid, I just added the red arrows just to highlight places that you can look

Segment Surveys — Tampering

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

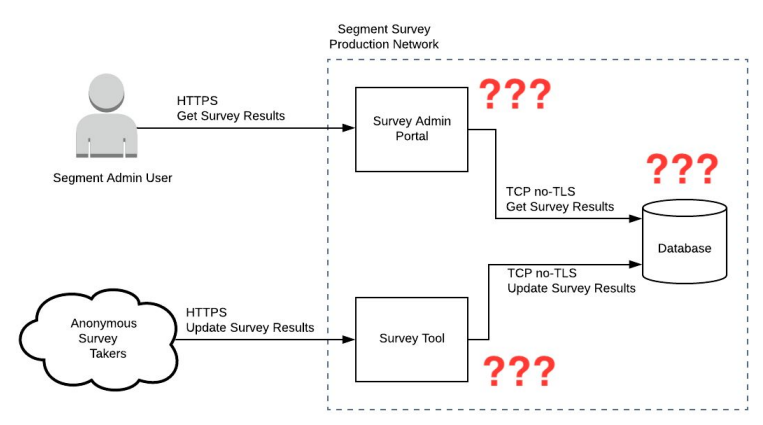


What are some tampering related questions that you may have?

- 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.



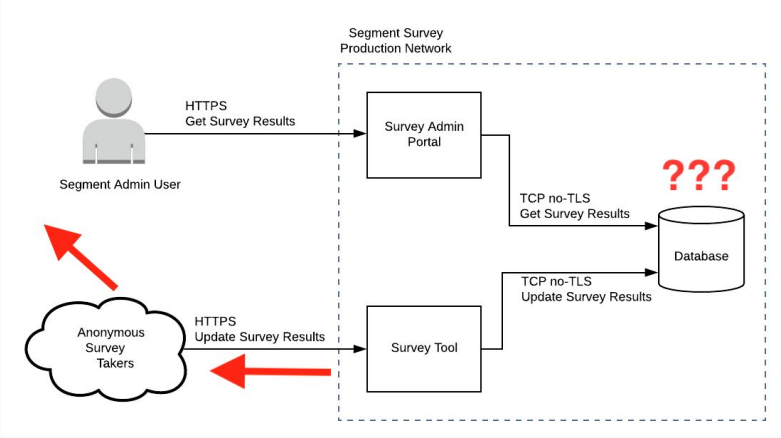
Changed the red arrows to question marks :)

What are some repudiation related questions that you may have?

- What information are we logging and where are we logging that information?
- Do we log access to the Survey Results application?
- Do we log login Segment Admin login requests?

Segment Surveys — Information Disclosure

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

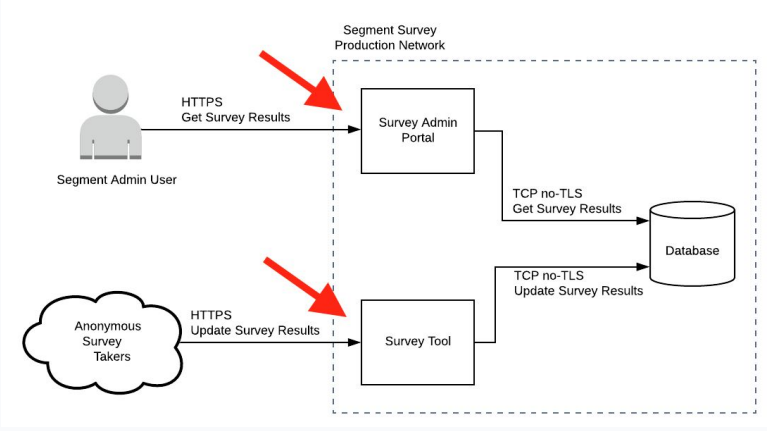


What are some information disclosure related questions that you may have?

- 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.

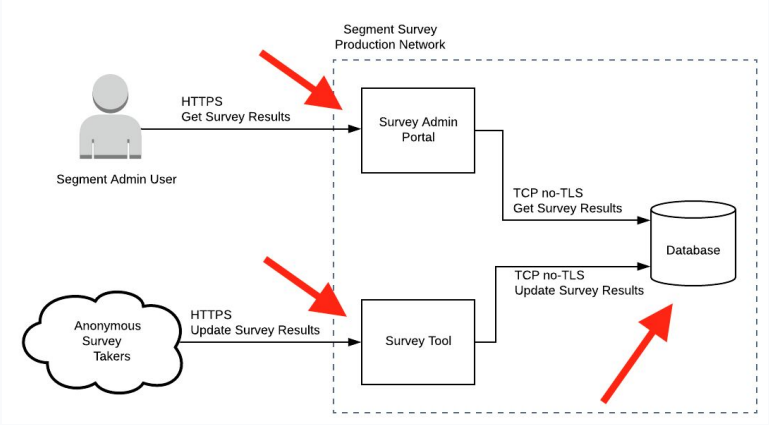


What are some DoS related questions that you may have?

- 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?

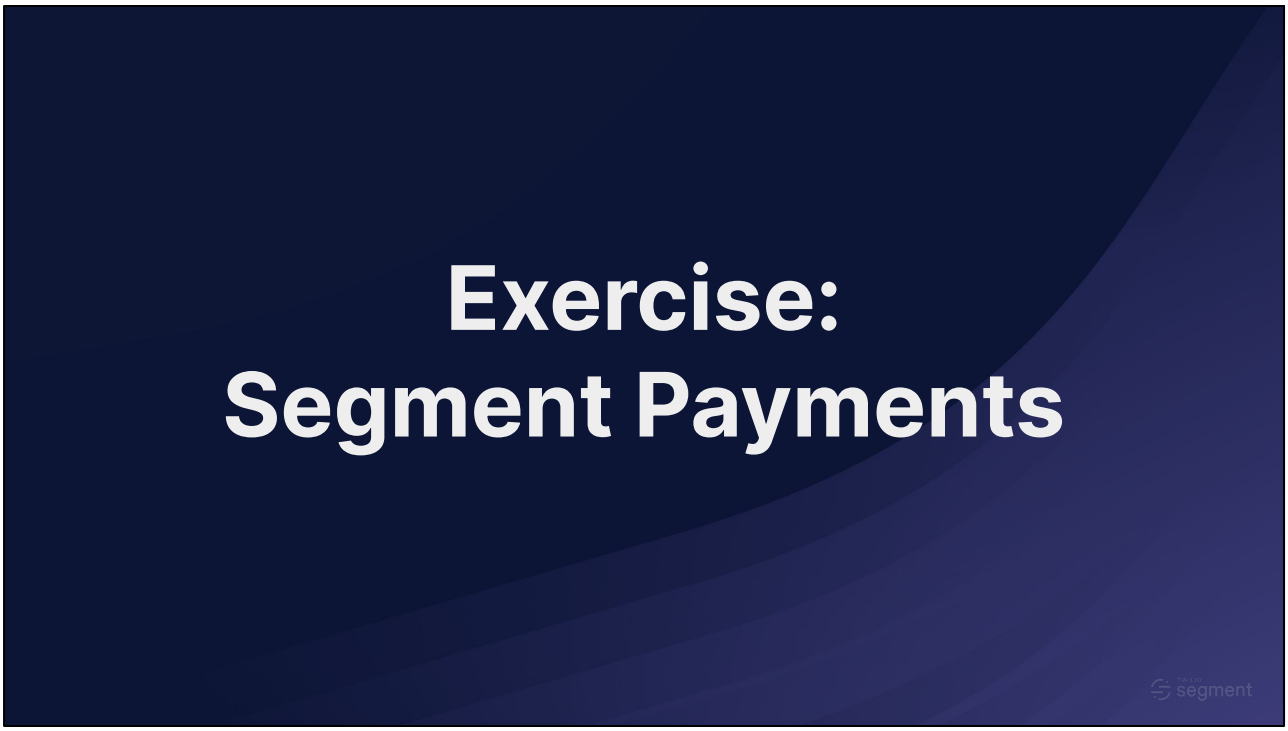
Segment Surveys — Elevation of Privilege

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



What are some elevation of privilege related questions that you may have?

- 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?



Alright, we have warmed up, now let’s get our hands dirty

Threat Modeling Questions

Let's do a bit more Threat Modeling.

- Review the SDD, it contains the feature breakdown
- Find risks and prioritize them
- Once done, we will discuss the threats and any other security questions or concerns that we have.

Read the slide

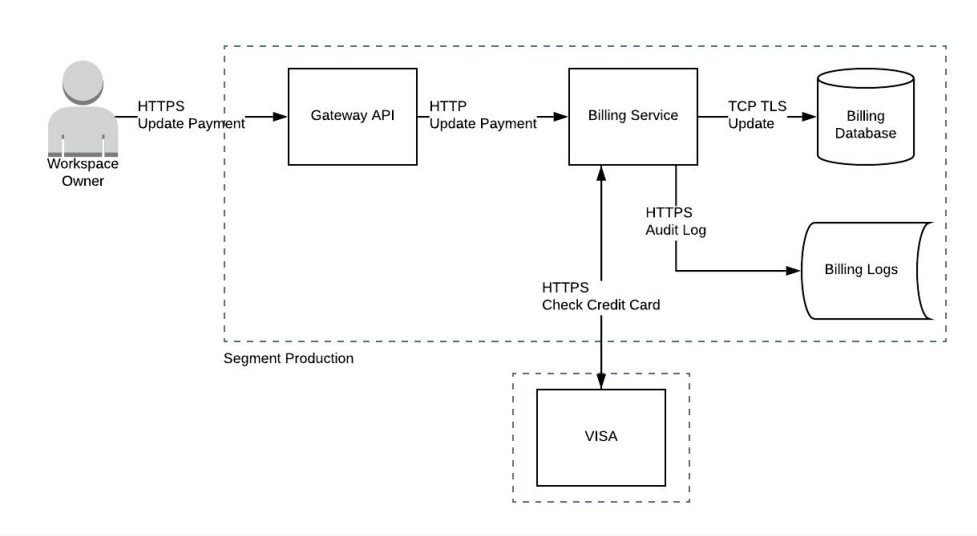
Update Payment API

To better serve our smaller clients, we now allow them to pay via Credit Cards. The Owner can add their Credit Card information in the UI, which calls the API.

Before updating the credit card on file, there would be a check with VISA to make sure it is valid. The system will also send the appropriate information (non-sensitive) to our secure Billing Logs.

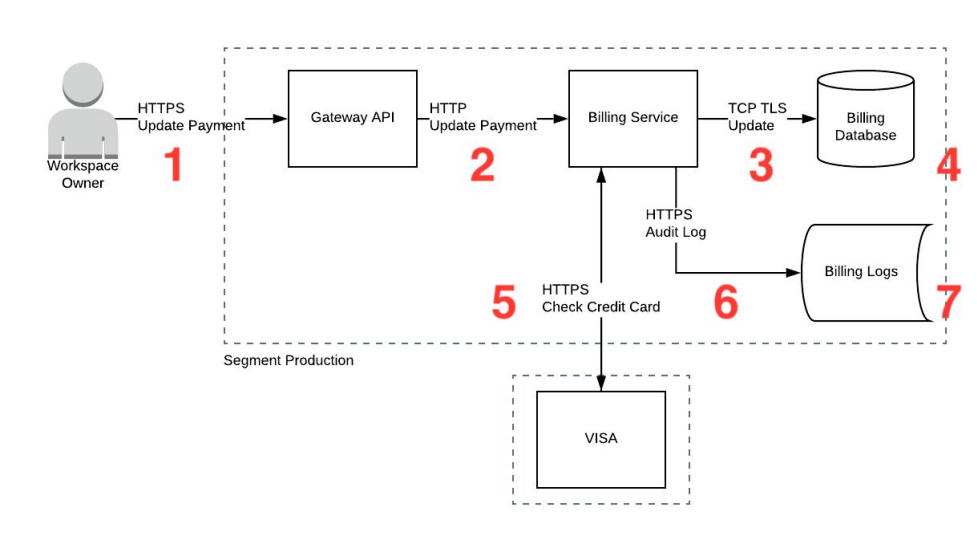
Read the slide

Update Payment Architecture



Talk about the different components of the architecture

Update Payment Architecture — Enumerate



The numbers are there to talk about the different areas that you can explore within this system.

1. Are there concerns between a Workspace Owner and the Gateway API?
2. Are there any threats between Gateway API and the Billing Service?
3. Do you have concerns between Billing Service and the database?
4. What are the concerns with the Billing Database?
5. Are there any concerns between the Billing Service and VISA?
6. Are there any threats between the Billing Service and the Billing logs?
7. Do you have any concerns with the Billing Logs?

Let the folks know that this information is also available in the SDD.

Breakout

We will break out into groups. We have the following goals:

- Review the feature breakdown
- Copy Example Template (at bottom of SDD) into your own shareable doc
  - 1 doc per group
- List your assets - you want to figure out what you are trying to protect
- Use STRIDE to find threats
- Prioritize your risks and we will discuss your top 3

Let's connect back in forty-five minutes.

TWILIO segment

We are working through the threat modeling workflow

- Breaking down the function (design doc)
- Finding Threat
- Prioritizing Threat
- Mitigating Threats (not done in this exercise)

There is an exercise template at the bottom of the design doc, just copy and paste that elsewhere.

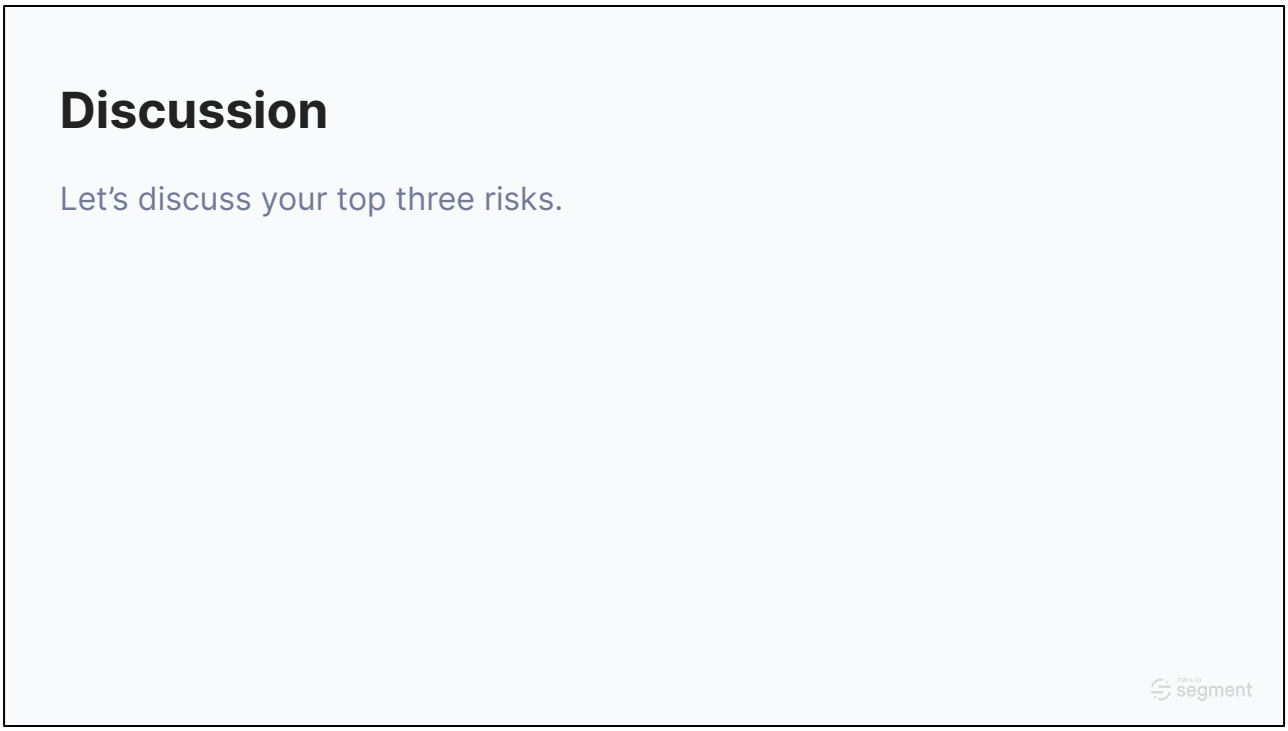
With respect to this exercise, we need you to:

- Read the design doc (10 mins)
- List your assets
- Find threats to your assets (30 mins)
- Prioritize the risks (5 mins)

Please keep track of all of your STRIDE threats in the template, it is easier to prioritize risks that way. There can be some ambiguous information, your job is to list assumptions or ask security questions.

We will talk about your threats when we all get back here in 45ish mins

Drop the link in:
https://github.com/segmentio/threat-modeling-training/tree/main/01%20-%20Payments%20Exercise



Each time to discuss their top three risks. Hopefully everyone has different risks, but there should be some overlap.

Note: If there is very little overlap, make sure to comment on diversity and how it has improved the threat model

An example Top Three Threats

1. Information Disclosure - As an adversary, I would create an account at Segment to check for legitimate credit cards, I might get a list of 10k credit cards and I want to validate which ones that I can use for fraudulent purposes - we should severely restrict changing credit card values
2. Spoofing - there was one mention of controls to DB, we restrict it to the Prod Admin role, is it possible for people with DB access to get credit card information. Ideally we don’t store any credit card information and we do it with a third party, let the third party assume the risk.
3. Denial of Service - Can I make 100 calls/minute and drain Segment’s bank account on making the same request over and over until I blow the month’s budget on this?

Phew,
almost done!

Goals

- Become more familiar with Threat Modeling
- Get our hands dirty with exercises
- Be comfortable asking security questions

Goals

- Ask the folks if they are more familiar with threat modeling now
- Did the exercises help you ask the right questions
- Are you ready for a live session?

TWILIO segment

You are now ready to try Threat Modeling!