Threat Modeling (222)
Optional Exercises

Table of Contents

Draw State Machine [optional]

Optional.	Due on:	Time Expectation:	15 – 30 min
	Private output, `state-bikes-$name.jpg`		

Context:

This exercise is focused on a state machine for the bikes themselves.

Instructions:

1. Create a new drawing. Call it `state-bikes-$name`
2. Create a state machine for the states of the bike
    a. The states should include at least rented, available and damaged.

Example:

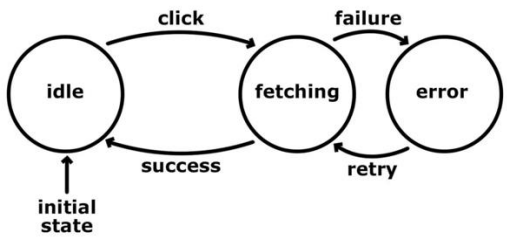


Diagram from https://albertodebortoli.com/2018/12/16/the-easiest-state-machine-in-swift/

Further reading:

https://online.visual-paradigm.com/diagrams/tutorials/state-machine-diagram-tutorial/
https://www.lucidchart.com/pages/uml-state-machine-diagram

Draw “Swim Lane” Diagram [optional]

Optional.	Due on:	Time Expectation:	15 – 30 min
	Private output, `swim-bikes-$name.jpg`		

Context:

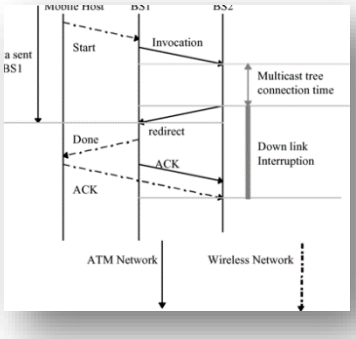
This exercise is focused on the network protocol used to sign up for the account, not perfection in the visual representation.

There are many forms of message diagram, including Swim Lane flowcharts, UML Message Sequence Diagrams, and more. Making nicely angled lines (left example) is a lot of work. Choose wisely.

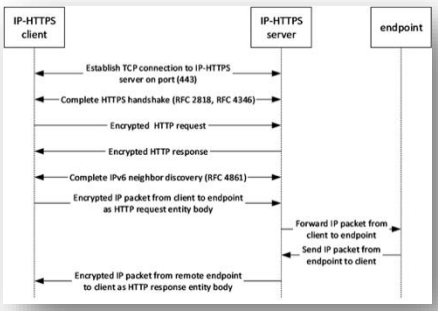
Instructions:

1. Create a new drawing. Call it `swim-bikes-$name`
2. Create a network protocol diagram for signing up for the app
    a. The protocol participants should include at least the app and the Bikes Cloud Service
    b. A sketch or two will probably help you.
3. If security issues occur to you as you work, take notes on them as a place to focus.

Examples



https://www.researchgate.net/figure/Hand-off-Protocol-packet-exchange_fig1_3812086



https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-iphttps/2762a506-f700-43cd-8798-751de36c2f1c

Further reading:

These may be useful inspiration https://www.eventhelix.com/networking/.

Trust Boundaries Essay II [optional]

Optional.	Due on:	Time Expectation:	30 – 60 min
	Private output, `essay-boundaries-ii-$name.txt`		

Context:

This exercise is focused on helping you see how trust boundaries relate to different diagram types. It has as a pre-requisite of at least one of the swim lane or state machine diagram exercises. If you've only done one, skip that step.

Instructions:

1. Create a new file called `boundaries-essay-ii-$name.txt`
2. Examining your state machine diagram, write at least a paragraph about where the security of the system changes. (Assuming you did that optional exercise.)
3. Examining your swim late diagram, write at least a paragraph about where the trust boundaries are in the system. (Assuming you did that optional exercise.)
4. Write at least a paragraph comparing and contrasting the trust boundaries.
5. Add a bullet list: What guidance or advice about trust boundaries would you give someone using a different diagram type?

Reconstruct Assumptions [optional]

Optional.	Due on:	Time Expectation:	15 – 30 min
	Private output, `assumptions-$name.txt`		

Context:

This exercise is focused on identifying the assumptions you've made in the steps so far, to help you understand why keeping track as you go is important.

Instructions:

1. Create a new file called `assumptions-$name.txt`. (Please follow the naming convention in case you choose to share the file.)
2. Consider your diagram(s), and ask yourself, "what assumptions did I make here?" "Where did I make a decision about the system" and "might I have made that assumption about real technology in a system I'm threat modeling if the author wasn't available?"
3. Repeat across other diagrams, including the trust boundaries and how they're enforced.
4. Go back through the document and consider how you'd test or validate each assumption. (It may help to convert to a spreadsheet or table.)

Construct an Attack Tree [optional]

Optional.	Due on:	Time Expectation:	15 – 60 min
	Private output, `attack-tree-$name.txt`		

Context:

This exercise is focused on crafting an attack tree, so that you can discuss from experience the challenges involved. The lowest effort and simplest approach is to record the tree as an outline. A sketch may help you visualize the tree and layers but avoid getting distracted by making the results pretty.

Instructions:

1. Create a new file called `attack-tree-$name.txt`. (Please follow the naming convention in case you choose to share the file.)
2. Draw an attack tree with a goal of getting a free bike ride.

Example:

1. Steal the customer database (goal)
    A. Attacks on cloud provider
        a. Break in, get command execution
        b. Access data stores
    B. Attacks on Bikes as a service cloud
        a. SQL injection
        b. API attacks
            i. Insufficient auth
            ii. APIs that give out information about who has which bikes?
        c. Backup and auth
        d. CI/CD pipeline

Why Now? [optional]

Optional.	Due on:	Time Expectation:	15 – 30 min
	Private output, `why-now-$name.txt`		

Context:

This exercise is focused on crystalizing the sense of urgency for changing the way your organization threat models.

Instructions:

1. Create a new file called `why-now-$name.txt`
2. Start with an event and talk about why it matters.
3. Tie that event to threat modeling explicitly
4. Explain any wins you've achieved
5. What's the goal?
6. Is there a timeline?
7. (Consider a few who/what/why/when/how statements.)

Example:

"The news of Solarwinds really shook our executive team. There's a lot of concern about the integrity of our build systems, and so we undertook a threat model for the CI/CD pipeline which identified 7 issues which were rapidly mitigated. There's a desire to scale that out and see where else we have such blind spots."

Hints:

If you're having trouble, consider:

- Events in the news (such as Solarwinds)
- Regulatory changes (TSA security guidelines for pipe operators)
- Priorities your executives are focused on
- Protoytpes or proofs of concept by your team, changes in capabilities

Roles and Responsibilities [optional]

Optional.	Due on:	Time Expectation:	30 – 60 min
	Private output, `role-responsibilities-$name.txt`		

Context:

This exercise is focused on crisply defining who does what within your organization. If you're not familiar with RACI, there is background material on the next page.

Instructions

1. Create a new file called `roles-responsibilities-$name`
2. Create a table with at least 5 rows and 5 columns.
3. Label the columns "Tasks", and roles in your organization.
4. Fill out the matrix to show who does what today.
5. Optionally, create a second aspirational (goal state) matrix.

Success is a matrix which represents your organization, and shows all the artifacts produced, and who produces them to the point where someone would say "yes, this is done properly" about the threat model.

Example:

Task	Developer	PM	SRE	Security	Engineering manager	Security center of excellence
Diagram creation	R	I	I	C	A	I
List threats	C	C	C	R		I
Bug filing						I
Evaluation						R

Hints

- The breakdown of both tasks and roles can vary with your specific practices.
- Consider tasks such as tracking and analyzes bugs, writing security tests

- Consider jobs and how they can participate: your security ops center, regulatory compliance teams, and others.
- There is additional (background) information on RACI on the next page.

RACI Background [optional]

RACI is a tool for showing who is responsible for what. It has 4 responsibility types:

- Responsible is the person who does the work
- Accountable is the person who ensures the work is done.
- Consulted are people who are asked for their opinion, input, or participation
- Informed are people who see the decisions, outputs, or deliverables, and are expected to take them into account.

Tasks are the specific activities to be done which produce an output artifact.

There are lots of RACI variants – if your organization uses something that's easily understood by other students in the class, please feel free to use it. If you had to take a training class to learn the system your organization uses, please use RACI for this exercise.

RACI Chart (Roles and Responsibilities Matrix)

For instructions / training material visit http://www.racichart.org

Process Name / Description:	*Plant maintenance project: Repair and resurface plant parking lot during plant shutdown in July*
Created On:	*1-Jan-16* Revision: *3/12/16*
Created by:	*Kelly Bradley (facilities mgr), Mike Cole (plant manager), Joe Pallino (HR), Brian Sullivan (security), Billy Ownens (project manager)*

	Facilities	Plant Mgr	HR	Security	Project Mgr
Identify a minimum of three asphalt contractors from Angie's List	C	-	-	-	R
Arrange for contractor visits and quotes	I	-	-	-	R
Review quotes and references, make contractor selection	A	I	I	-	R
Review and finalize contract, lock in plant shutdown week	I	I	-	-	R
Communicate project to shutdown maintenance crew, make sure all vehicles are removed from the lot	I	I	R	I	I
Provide security gate access codes for asphalt crew by June 15	I	-	A	R	I
Oversee the project during the plant shutdown week, ensure it is completed on time	A	I	I	-	R

R = Responsible, A = Accountable, C = Consulted, I = Informed

There's plenty of good stuff on RACI on the internet if you want supplemental reading.

Consider Who Cares? (Essay) [optional]

Optional.	Due on:	Time Expectation:	30 – 60 min
	Shared output, `who-cares-$name.txt`		

Context:

This exercise is focused on understanding who cares about changing the way your organization threat models.

Instructions:

1. Create a new file called `who-cares-$name.txt`
2. Start with the person who is responsible for you taking this course and explain why it matters to them.
3. Iterate through the people that influence that person
4. If you can include exact quotes, that will help you
5. List the people who you expect to be opposed to or resistant to threat modeling, and why
6. Ideally, both lists will contain both executives and respected technical leaders.

Example:

Bob sent me to threat modeling training because we are trying to be more structured in how we think about the security of our operational systems. That matters to Amy, VP of operations, because she wants fewer projects hitting snags or getting escalated. She also sent Bob, who's one of her key staff folks.

File information:

9-exercise-compliation-222-extended-3.docx last printed 8/15/2022 1:31:00 PM

License: