Agile Threat Modelling
WORKSHOP GUIDE

On agile software projects, it is important to distinguish between the activity of *threat modelling* and the final artifact, which would be a *threat model*.

Waterfall approaches to threat modelling focus on the artifact - a detailed system model and an exhaustive (*exhausting?*) list of threats, vulnerabilities and attack trees. The feedback when we try waterfall threat modelling on agile projects is usually the same - "Takes too long" , "Too hard", "We never finished!" and "Not valuable!"

Our goal instead is to find the highest value security work we can do, and get it into the team's backlog right away. We do this by applying a timebox so we are threat modelling *"little and often"*. We capture a new and different *partial view* of the system each time we do threat modelling rather than overthinking it. Over time, we try lots of perspectives and zoom levels on the system- threat modelling becomes an agile *continuous process*!

Preparation

- Timebox the activity - do not plan for more than 1 hour and 30 mins - aim to finish on time.
- Once the team has the muscle memory of threat modelling much shorter sessions will work
- Remember, ***"little and often"***
- Gather the team around a whiteboard, in a meeting room to start
- Make sure someone on the team is able to draw some diagrams
- Invite product owners and security team folks to get a rounded perspective.

You will need:

- STRIDE Cue Cards
- Whiteboard
- Whiteboard pens
- Stickies
  - Square ones
  - Tiny ones
- Sharpies
- Time: 1-1.5 hours

Agree on scope ahead of time: Agile threat modelling works better with small aspects of a system such as a login page, a new user flow, an email sent to users or a single user story. Try these kinds of focus rather than trying to bite off the entire system at once.

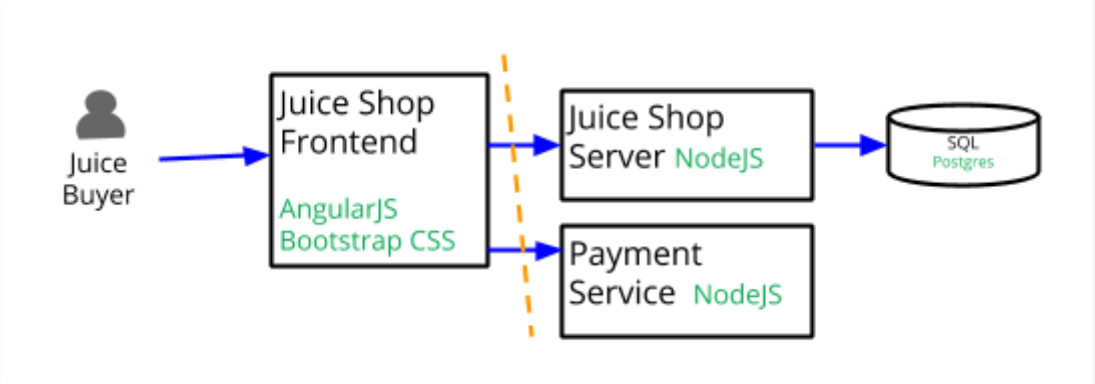
Alternately, model a subsystem - say the delivery pipeline, a microservice, the identity system or part of your infrastructure. If you are trying this for the first time, a broad brush overview of the system to review security debt can be a good way to kickstart the practice.

Limit granularity - remember you only have at most 1hr and 30 minutes! Prioritise by risk.

What are we building?

Developers are comfortable with drawing diagrams to represent systems, for example sharing technical vision or exploring technical designs outside of the-security context. So use these established skills! The activity should be familiar, but with a few threat modelling extras.

Ask participants to draw technical diagram of agreed scope [10 mins]



People usually start by drawing boxes or circles for components - great

Use triangles or people icons for users

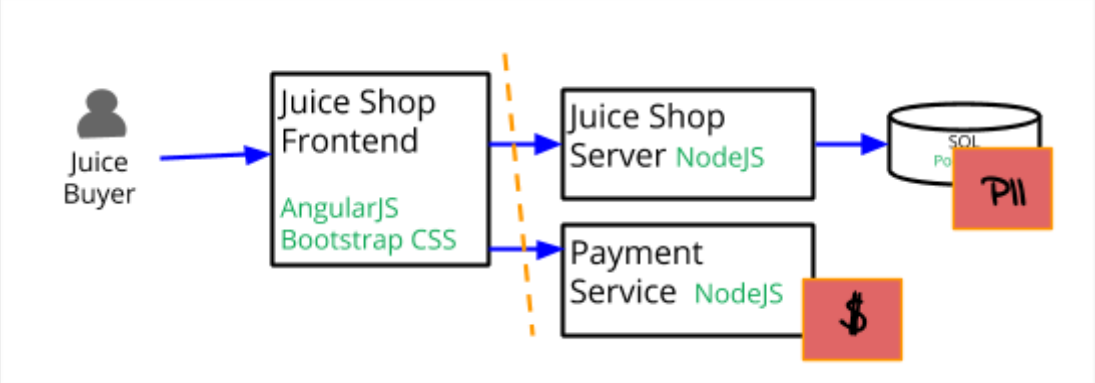
Most data flows are bi-directional, draw arrows **from where they originate**

Draw data flow arrows in different colour so they stand out

Sometimes data flows cross authorisation boundaries: login, firewall, service authentication etc.

^^ Add these as dotted lines in another colour

Highlight what (data, services, assets) we need to protect [2 mins]



Don't be exhaustive!

Timebox highlighting activity to 2 mins

With bright stickies, tag your valuable "things". Your prized assets- it might be a service or it might be data

E.g. 1. Personal data (PII) in the customer database or
2. Service itself which needs to be available ($).

What can go wrong?

The next activity is ***"Evil Brainstorming".*** Folks may not be familiar with this kind of thinking. We are going to use STRIDE as a guide, a well established and effective methodology.

With newcomers the terms in STRIDE are slippery. Get participants to read the cue cards out loud and discuss the concepts. Check that all of the words and concepts are understood by the team.

Brainstorm threats: use STRIDE cue cards [30 mins]

Hand out the cue cards to the participants, perhaps give one each or between two

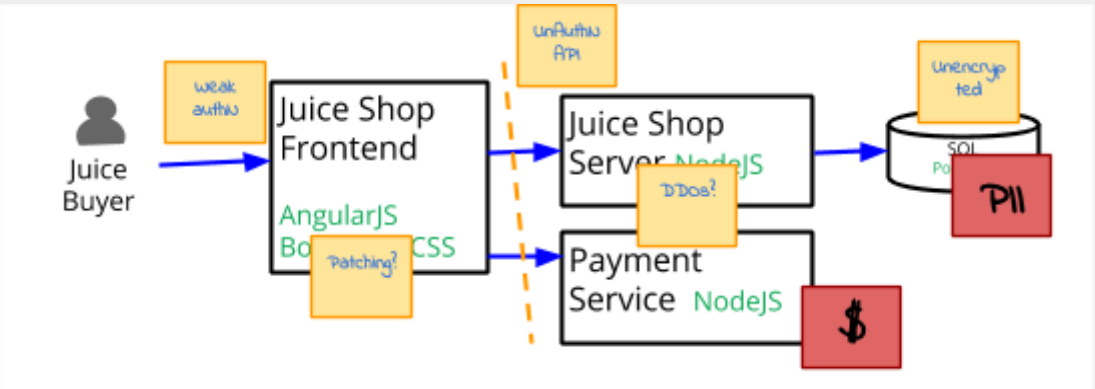
Goal is to brainstorm as many **potential threats** as possible, *quantity over quality!*

Do not explore risk (likelihood, impact) or controls (how to safeguard) yet - *these are rabbit holes!*

We will use the STRIDE framework to help brainstorm threats, one cue card at a time

Start by asking someone to read the content on the front of the 'Spoofed Identity' card

Follow the dataflow lines! Can we brainstorm any threats for this cue card?



For each threat (*particular vulnerability or missing safeguard*) note it on a sticky.

Tag the sticky onto the specific spot on the diagram where it applies

For each STRIDE card, brainstorm threats using content of cards as a cue

Note: STRIDE is for brainstorming not classification, so don't worry if a sticky is an example of 'Spoofed Identity' and 'Escalation of Privilege'- that is not a problem! Just brainstorm potential threats!

What are we going to do about it?

Now we have completed our brainstorm we need to *prioritise* and make sure the outputs are *actionable*. Capturing actions is the *most important* but least fun part of Threat Modelling: but as facilitator your role is to ensure actions are captured otherwise the team's time has been wasted.

Prioritise by voting for riskiest threats [10 mins]

We will now prioritise according to **risk**

We do not have unlimited bandwidth to work on every single threat right now

Risk is about how likely the threat is to happen and also what the impact might be

People have an intuitive sense of risk and should be able to cast their votes with minimal prompting

Cue: Do we have evidence of a threat? Did we see it before? Is it common (such as OWASP top ten)?

Cue: How exposed is any vulnerability? On the public Internet? Exposed to all users? Only admins can exploit?

Cue: What is the worst case scenario? Could the vulnerability be combined with others to make it worse? What is impact?

Everyone gets 3 votes (use sharpies or small stickers). Folks can vote on the same threat more than once if they like.

Take a photo of the diagram, the threats and the votes [1 min]

Take a photograph using a mobile phone camera at this stage, to capture the output of the brainstorming and prioritisation. Upload it to your Wiki or planning tool.

Take top three threats define actions and add to backlog [20 mins]

Outputs must be in format the team can process: **in the delivery backlog**.	Identify the **three stickies** with the most votes and discuss each one in turn	Specify *one or more* actions to **mitigate** for each of the stickies
Output can be **security debt** which can be tracked via your tech debt process	TECH DEBT: Review cloud network security rules to make sure they are not overly permissive to protect against escalation of privilege by attackers on the Internet	
Output can be **additional Acceptance Criteria** on an existing user story	ADDITIONAL ACCEPTANCE CRITERIA: GIVEN the threat from users tampering with input WHEN validating a comment provided by the user THEN reject any attempted XSS	
Output can be changes to the team's **definition of done**	DEFINITION OF DONE No story making changes to unauthenticated APIs accessible from the Internet will be accepted without exploratory security testing due to threat from tampering with input and escalation of privilege	
Output can be **timeboxed spikes** to determine if we are really vulnerable	SPIKE: SQL injection into backend The possibility has been raised that XSS in delivery notes section might get passed through to legacy system and impact call centre. This spike is to investigate.	
Output can be **extra Epics** to implement significant security safeguards	EPIC: Security Logging AS A regulated business in the finance industry WE NEED an infrastructure for aggregating and reporting on audit events generated by the frontend of the system SO THAT we protect against the threat of financial loss due to repudiation of action by fraudsters making payments	

Congratulations! Workshop is complete [1 min]

Thanks everyone for taking part in workshop! Hope you enjoyed it

Until next time!

Make sure any scope you defined as part of workshop is added to backlog

You can write up session using the Wiki Template

How do we know that we did a good job?

Perform a review of actions after 30 days
Are the actions complete? If not why not?
Time to threat model again!