LINDDUN GO

Getting started guide

LINDDUN GO
Getting started

Each threat modeler takes turns drawing a card from the draw pile and assesses whether the threat example is applicable to the system. When the threat modeler identified a first applicable threat, the other threat modelers join in to identify all other applicable threats.

READY?

Gather a group of threat modeling enthusiasts (2 to 5 participants).

Have or create a model of the system (a DFD-alike model is preferred, but a client-server view or even a white board sketch will do the job too). Make sure it contains at least elements that correspond to the hotspot types used by LINDDUN GO *(inbound communication, outbound communication, processes, storage and retrieval actions)* as you will need to iterate over each of these in the next steps.

SET?

Have a pen and piece of paper ready to document the threats. You can use the LINDDUN GO threat template, if you like.

Assign a secretary that will document the threats (who writes down what is being elicited).

Shuffle the Threat Cards and make 1 Draw Pile.

GO!

The first threat modeler draws a card from the Draw Pile and tries to identify an applicable threat w.r.t. the drawn card. Each card consists of the elements listed in Figure 1.

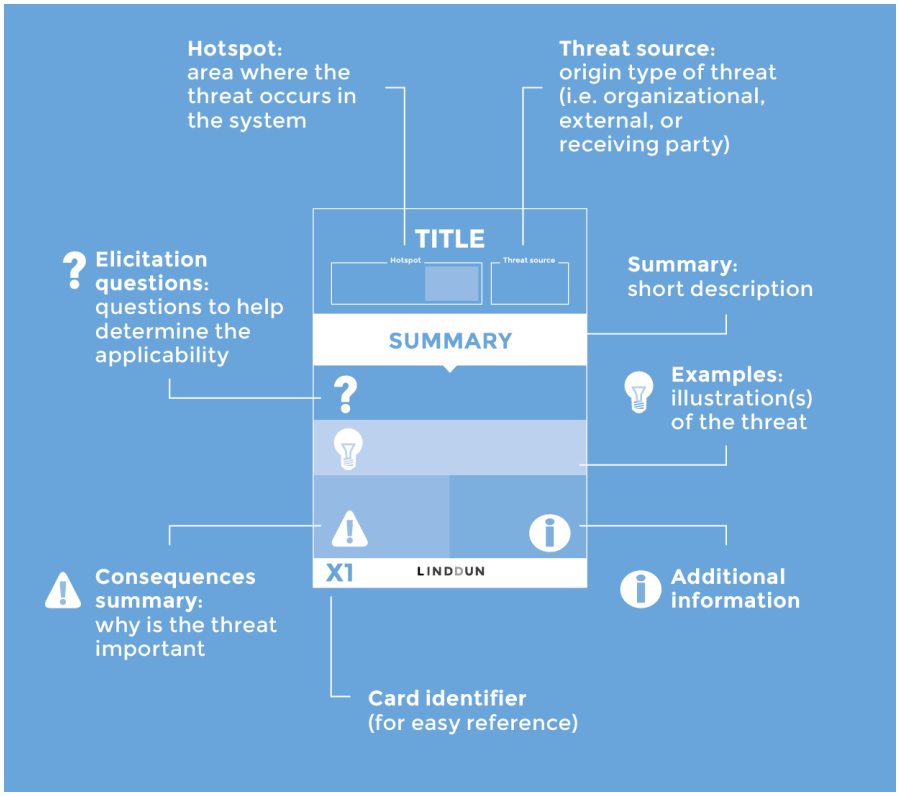


FIGURE 1: THREAT TYPE CARD SUMMARY

1. **Determine whether the threat type described on the drawn card corresponds with an applicable threat for your system.**

   ### How to elicit a threat using LINDDUN GO card

   For each of the system's corresponding hotspot(s),
   you assess the following questions:

   - Q1 - Could it be done?
     - If the answer to the first question is *yes*, the prerequisites are fulfilled. *(if unsure, assume the answer is yes)*
   - Q2 - Would it be a problem?
     - If the answer to the second question is *yes,* it is considered a threat.

2. **You have found a threat.** Great! Document it by writing down the hotspot and threat.

3. **Take turns to find all threats related to the card.** When the threat modeler who drew the card found 1 threat (or decides they cannot find an applicable threat), the other threat modelers can fill in any overlooked threats. Work clockwise. Each threat modeler can identify one overlooked threat per round. Continue until you have completed an entire round with no new threats.

Note that the threat modeler who drew the card can also join in as they might have gotten inspired by the discussion with the other threat modelers.

Put the Threat card on the Discard pile.

The next threat modeler (the one to the left of the previous card drawer) can draw a card now.

FINISH

Continue until there are no more cards on the Draw pile. Congratulations! You completed the threat elicitation exercise.

Alternatively, you can also time-box the threat elicitation exercise and pick it up at a later time. In that case, make sure you mark the Discard and Draw piles and keep your documented threats at hand for a next round.

TIPS & TRICKS

- Discard non-applicable hotspot cards in advance or on the spot, i.e. when you draw a card with a hotspot that does not apply, you can discard it and pick a new card.
- When you take turns to identify additional threats that correspond with the drawn card, you might end up with a joint group discussion (rather than taking turns). This is of course also fine. Just make sure everyone is able to pitch in.
- Don't forget to shuffle the cards before you begin! The random order might inspire you to threats you might miss when you go through the deck category per category.
- With a larger group (4+ people) it can be useful to assign 1 person as moderator to coordinate the elicitation discussion.
- In addition to the card deck used to randomly select a threat type card, you can have additional deck(s) at hand as reference material for the other participants to read along.

ALTERNATIVES

Quick - Only the card drawer elicits an applicable threat. No group iteration over each card. Once the card is handled by the card drawer, it is put on the discard pile. It will likely result in a less complete set of threats but will keep more flow in the elicitation.

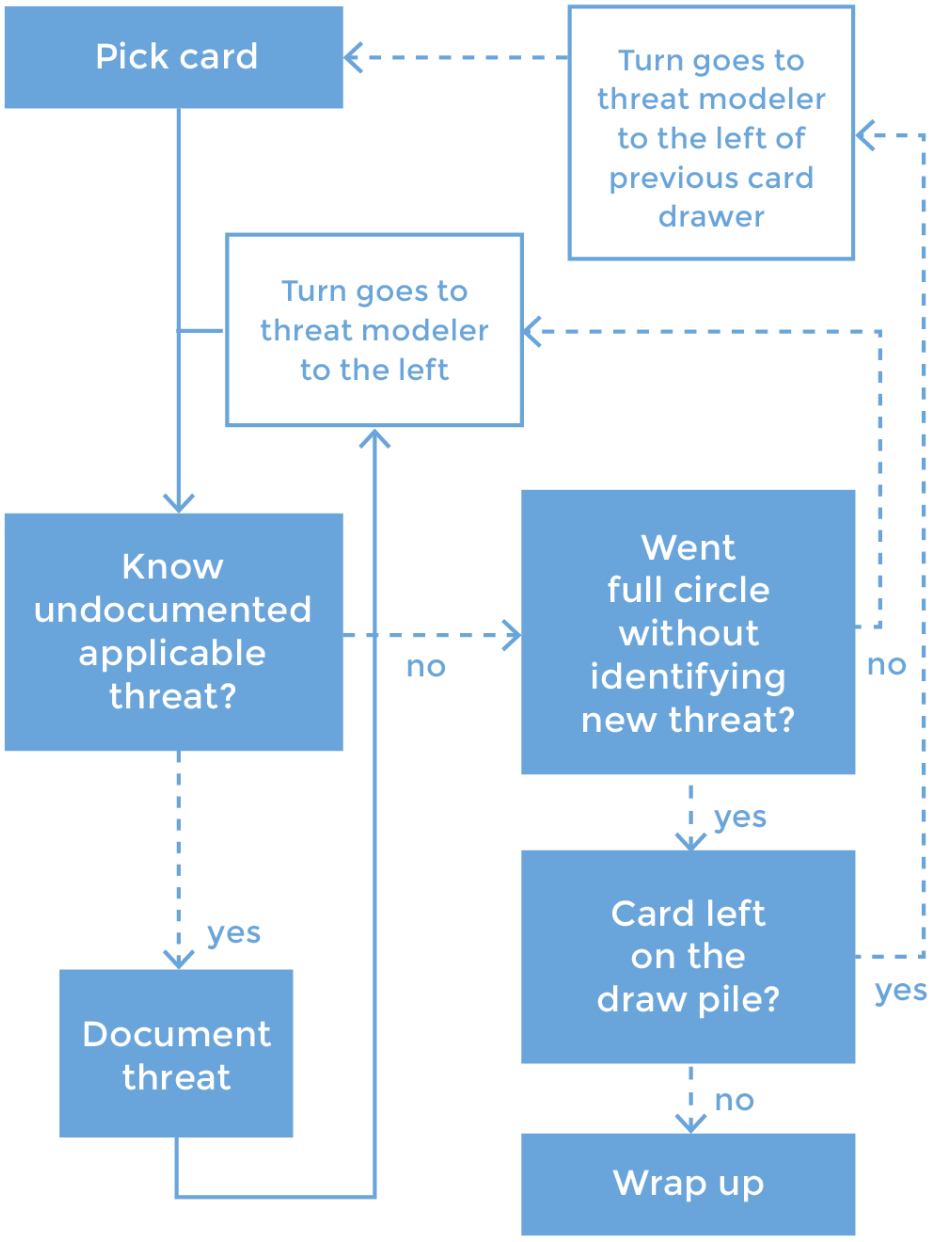
Time-boxed - Time-box the exercise (or limit the number of cards) and do multiple threat modeling sessions. As this threat modeling process can still take quite some time when discussing each card in group, it might be useful to have multiple sessions. Make sure to mark which cards were already covered (discard pile) and which ones you still need to examine.

Fun - Turn it into a game and earn points for each identified threat. If you like to include a playful element, you can make it a competition. Suggestion for scoring: count one more point than the points earned for the previously identified threat of the same card (i.e. first identified threat is worth 1 point, second 2, etc.).

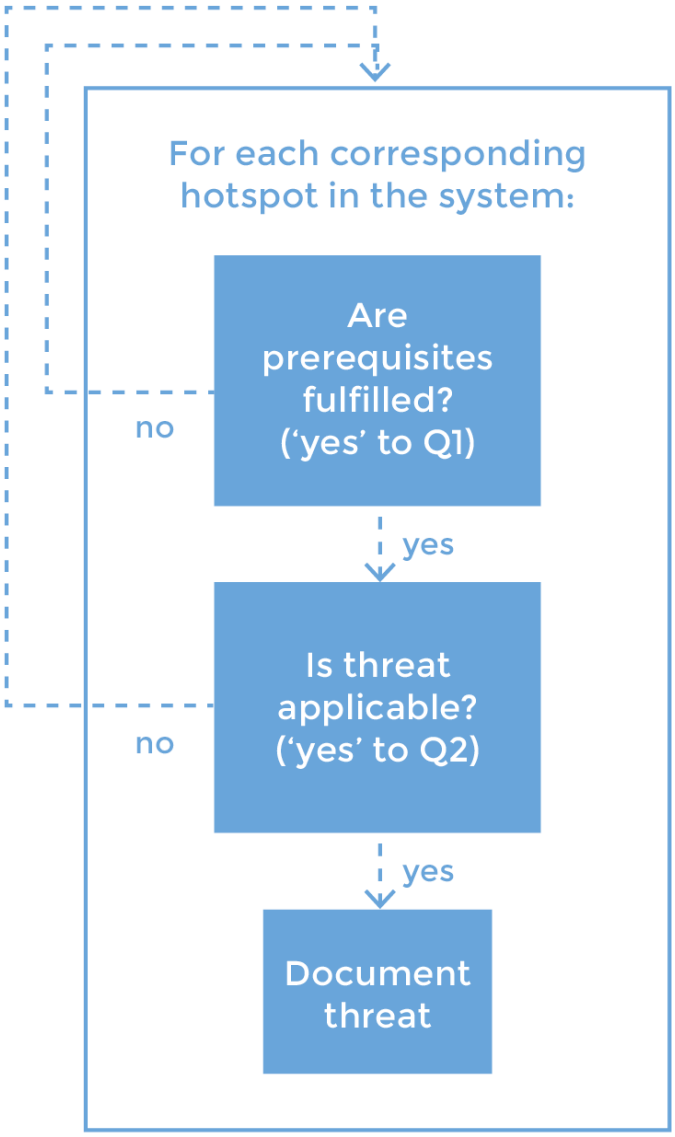
Solitary - use the threat type cards as input for an individual privacy threat elicitation exercise. Although LINDDUN GO was designed to be applied in group, the cards can obviously also be used by a single threat modeler as privacy knowledge base.

Freestyle - Only use the LINDDUN GO category cards to ideate privacy threats. Rather than using the threat types cards to elicit privacy threats, only focus on the main LINDDUN GO categories. *Note that this requires sufficient privacy expertise to be executed successfully.*

INSTRUCTIONS



HOW TO ELICIT A THREAT?



* if unsure, assume 'yes'

LINDDUN GO