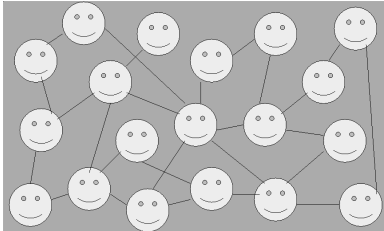# Activity: Threat Modeling with the Security Cards

Instructions: Read the description of the system and answer the questions below before you start the exercise with the Security Cards.

Koreshky via Wikimedia Commons. Public domain.

A Social Network

You work for a company building a new online social network (a competitor for Snapchat, Instagram, and Tumblr). It's designed to allow people to communicate with each other, on the website or via mobile apps. It has standard features like the ability to post photos, videos, and notes, and chat features so people can talk to one another one-to-one or in groups of up to 250 people.

1. Who comes in contact with the system? Think about who uses the system, who designed and made the system, and who makes decisions about how it works.

2. What data is involved? Think about what data is generated, what data is entered, and what data is collected.

3. Who can make changes to the hardware, software, and settings that govern the system?

4. How will the system components and the technology interact with the offline world?

Activity: Threat Modeling with the Security Cards

Instructions: Read the description of the system and answer the questions below before you start the exercise with the Security Cards.

A Self-Driving Car

Steve Jurvetson via Flickr. CC BY 2.0. Modified.

You're part of a new division at a major car company, designing a self-driving car (AKA driverless car, autonomous vehicle). The car uses a combination of cameras, radar, other sensors, and artificial intelligence to travel between destinations without a human operator. Self-driving cars have GPS systems, and they may also have 5G mobile connections to connect to various services via the Internet, as well as ways to connect and communicate with nearby vehicles.

1. Who comes in contact with the system? Think about who uses the system, who designed and made the system, and who makes decisions about how it works.

2. What data is involved? Think about what data is generated, what data is entered, and what data is collected.

3. Who can make changes to the hardware, software, and settings that govern the system?

4. How will the system components and the technology interact with the offline world?

Activity: Threat Modeling with the Security Cards

Instructions: Read the description of the system and answer the questions below before you start the exercise with the Security Cards.
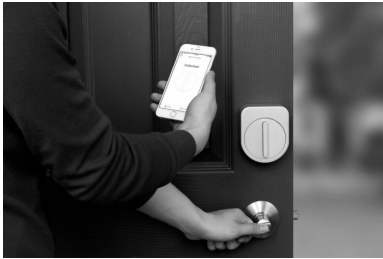
Scott Lewis via Flickr. CC BY 2.0.

A Smart Lock

Your company's smart lock replaces physical keys with a smartphone app. Someone installs a new lock, or adds new hardware to the current deadbolt, and installs an app on their smartphone. Then they can use the app on their smartphone to lock and unlock the door, monitor who enters and leaves through the door (using their own phones), and lock and unlock the door from anywhere they have an Internet connection.

1. Who comes in contact with the system? Think about who uses the system, who designed and made the system, and who makes decisions about how it works.

2. What data is involved? Think about what data is generated, what data is entered, and what data is collected.

3. Who can make changes to the hardware, software, and settings that govern the system?

4. How will the system components and the technology interact with the offline world?

Activity: Threat Modeling with the Security Cards

Instructions: Read the description of the system and answer the questions below before you start the exercise with the Security Cards.

An In-Home Voice Assistant

An in-home voice assistant (AKA virtual assistant, smart device, home automation hub) is a computing device connected to the Internet that responds to voice commands. Your company's smart home assistant will be even smarter than Siri, Alexa, or the Google Home assistant. These devices wait until they hears a "wake-word" (like their name) and then respond to voice commands to do things like play music, make to-do lists, set alarms, answer voice-based search queries, or provide weather updates.

Daniel Cardenas via Wikimedia Commons. CC BY-SA 4.0.

1. Who comes in contact with the system? Think about who uses the system, who designed and made the system, and who makes decisions about how it works.

2. What data is involved? Think about what data is generated, what data is entered, and what data is collected.

3. Who can make changes to the hardware, software, and settings that govern the system?

4. How will the system components and the technology interact with the offline world?