CSCI 476: Computer Security

Lecture 1: Introduction, Syllabus, and Logistics

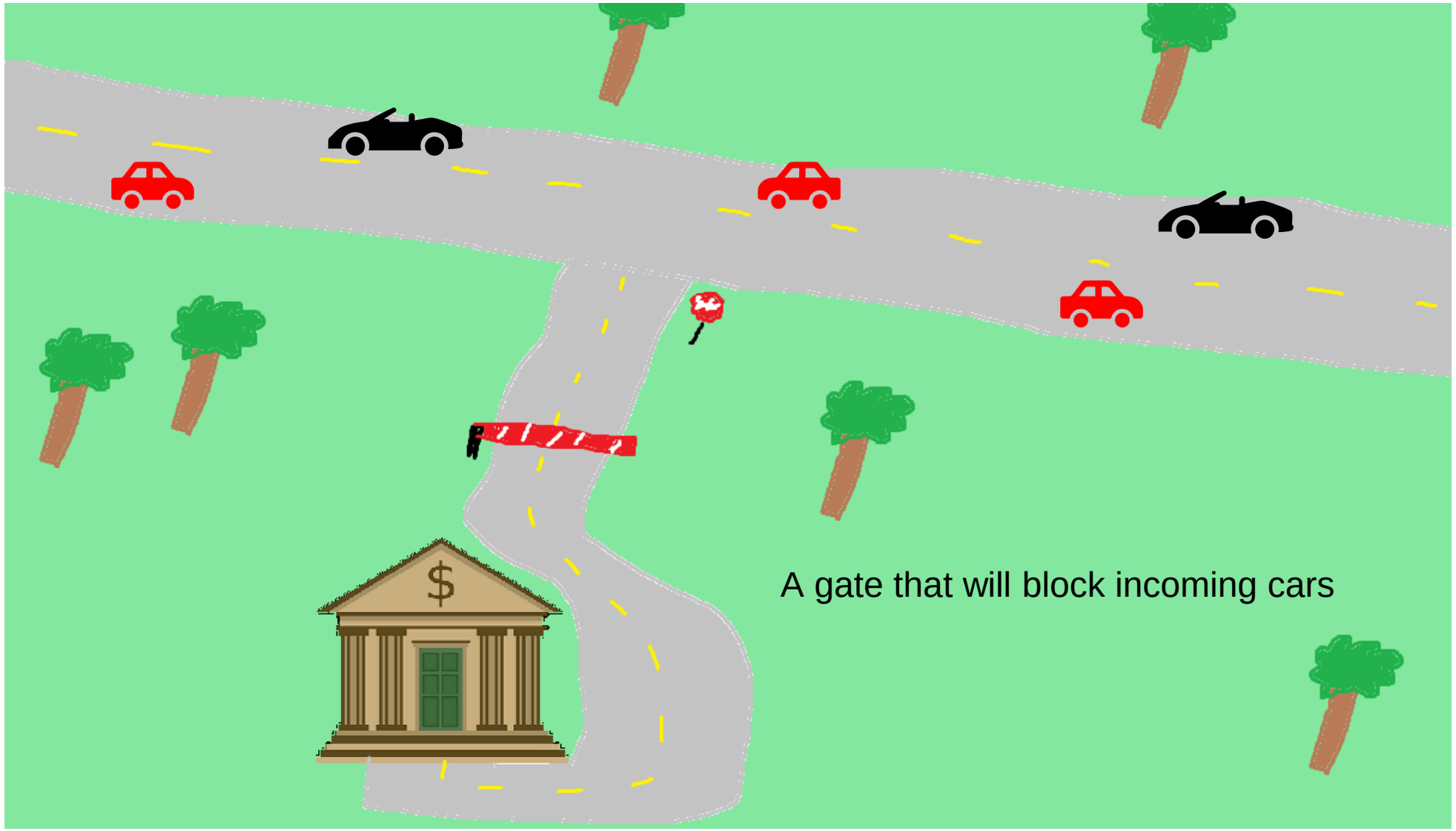
Reese Pearsall

Fall 2023

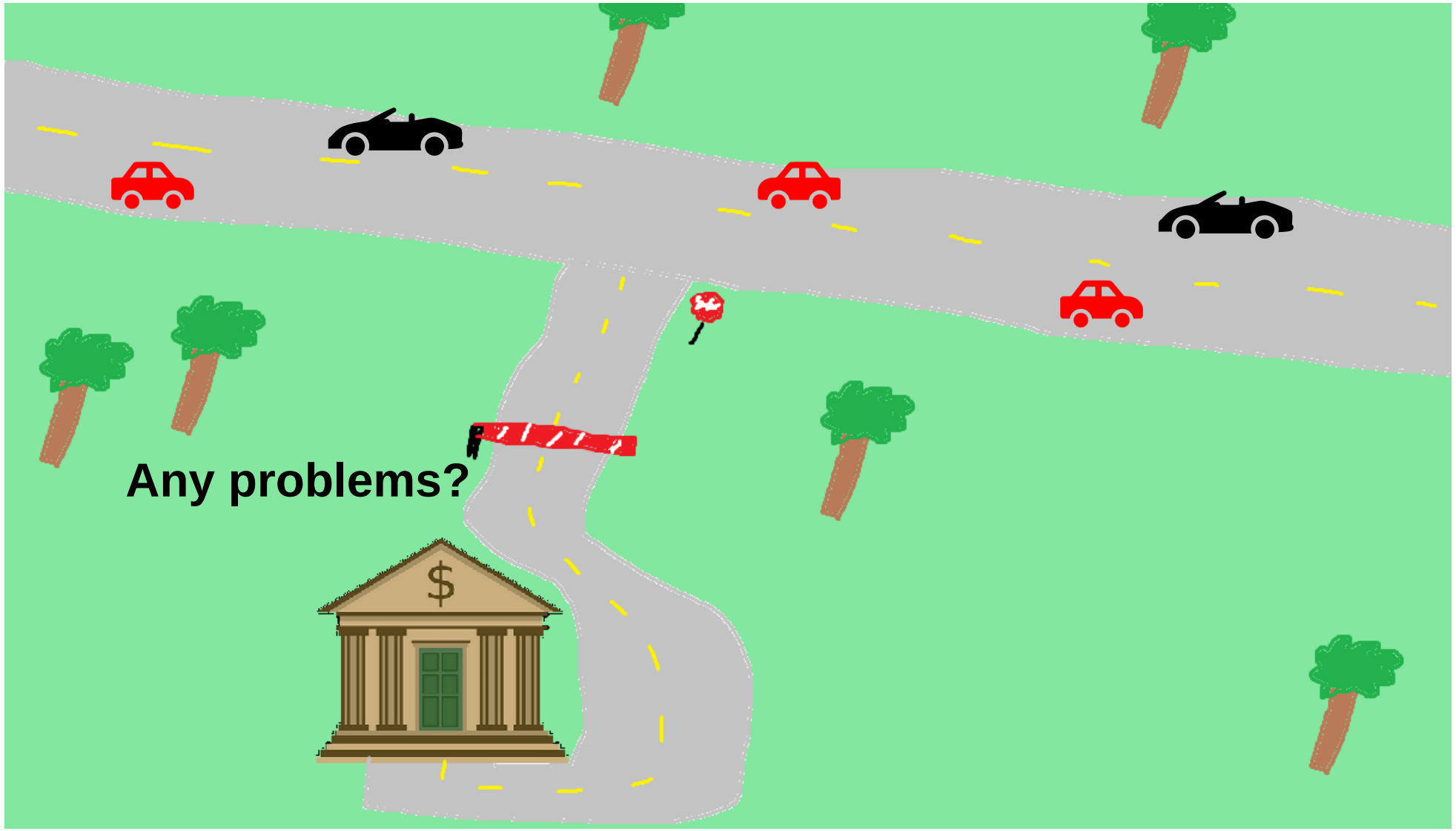
Before we jump into course rules, we will do a short exercise to get you thinking about security

Securing an asset

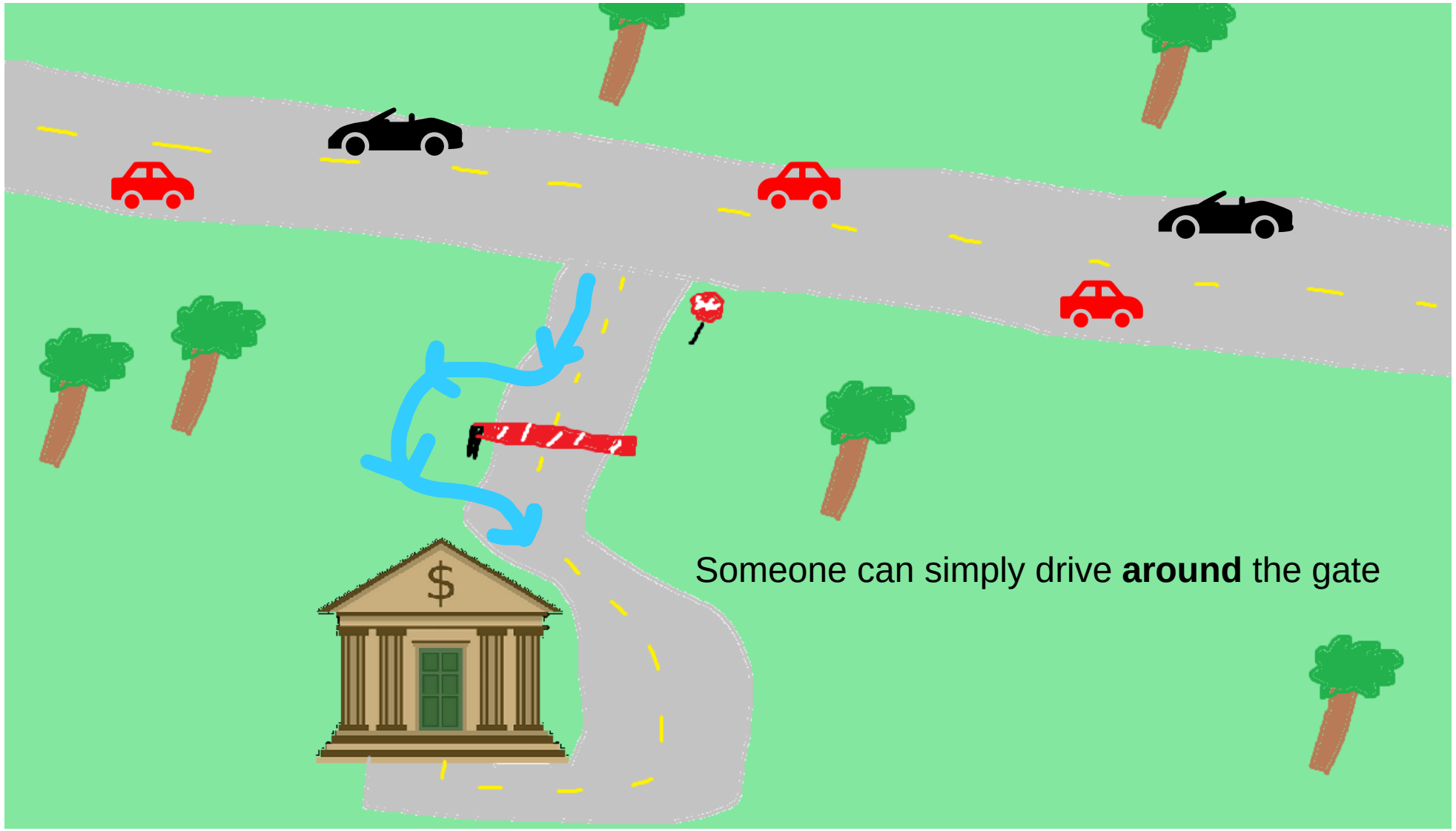
Securing an asset



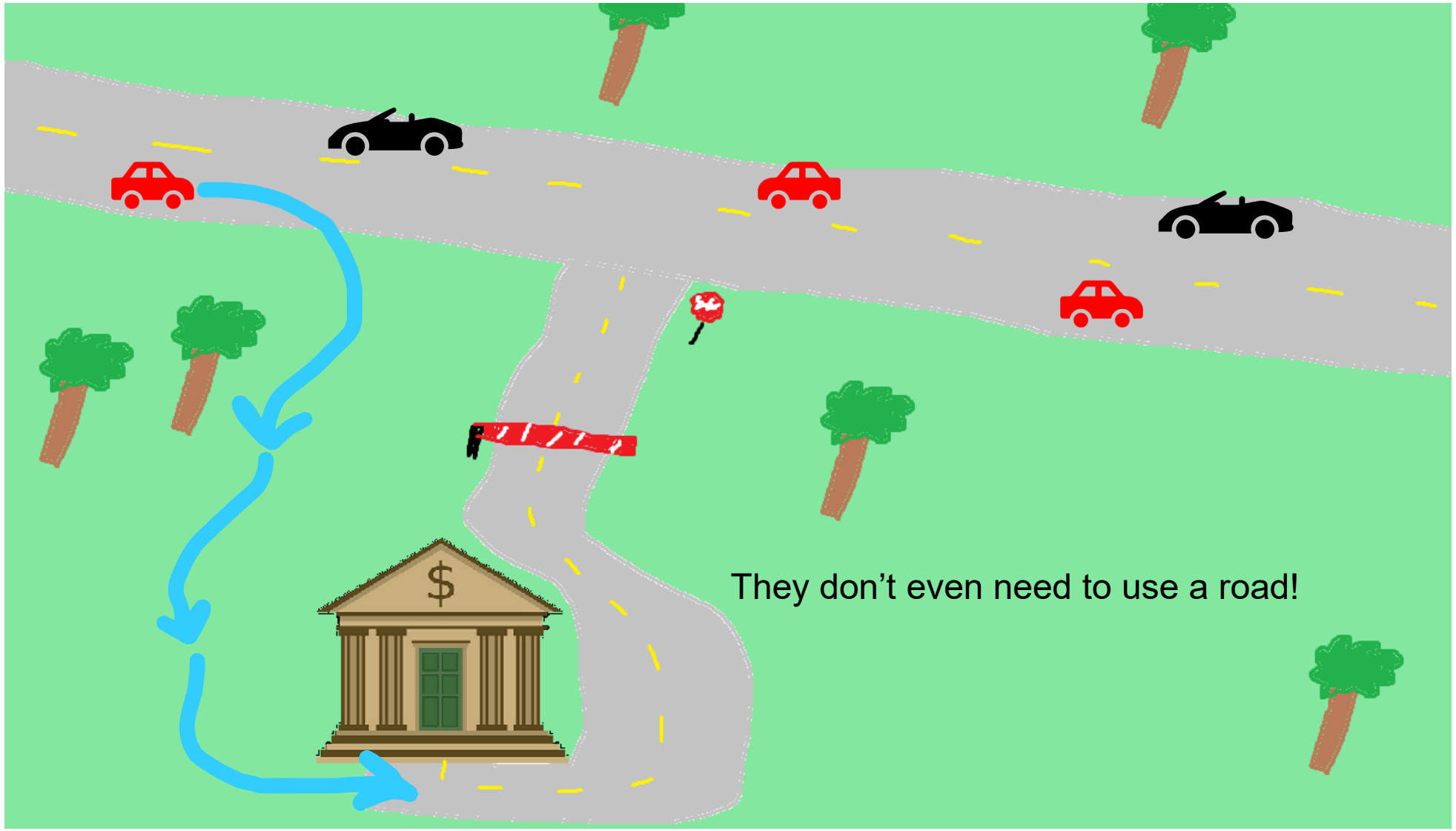
Securing an asset



Securing an asset



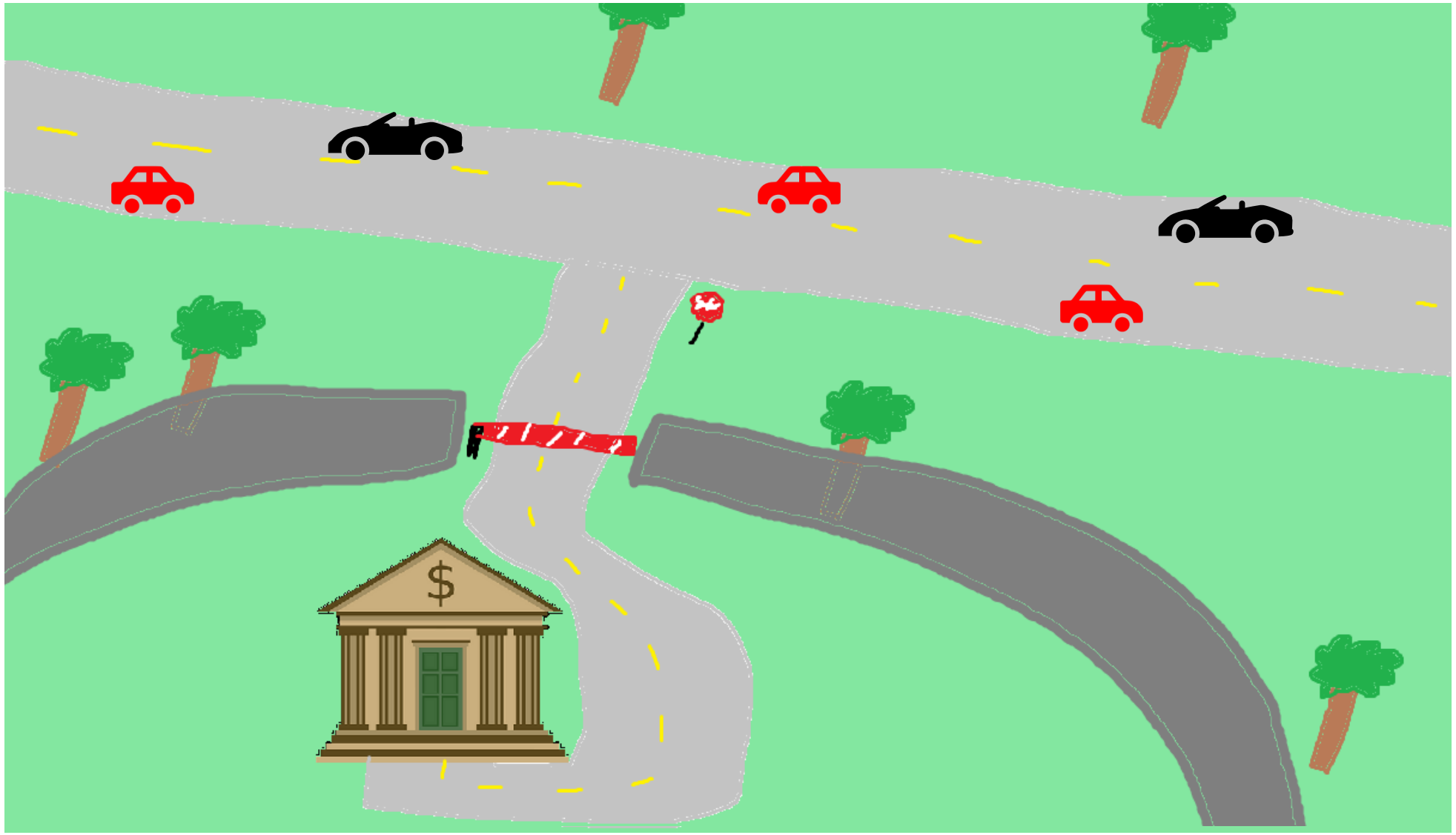
Securing an asset



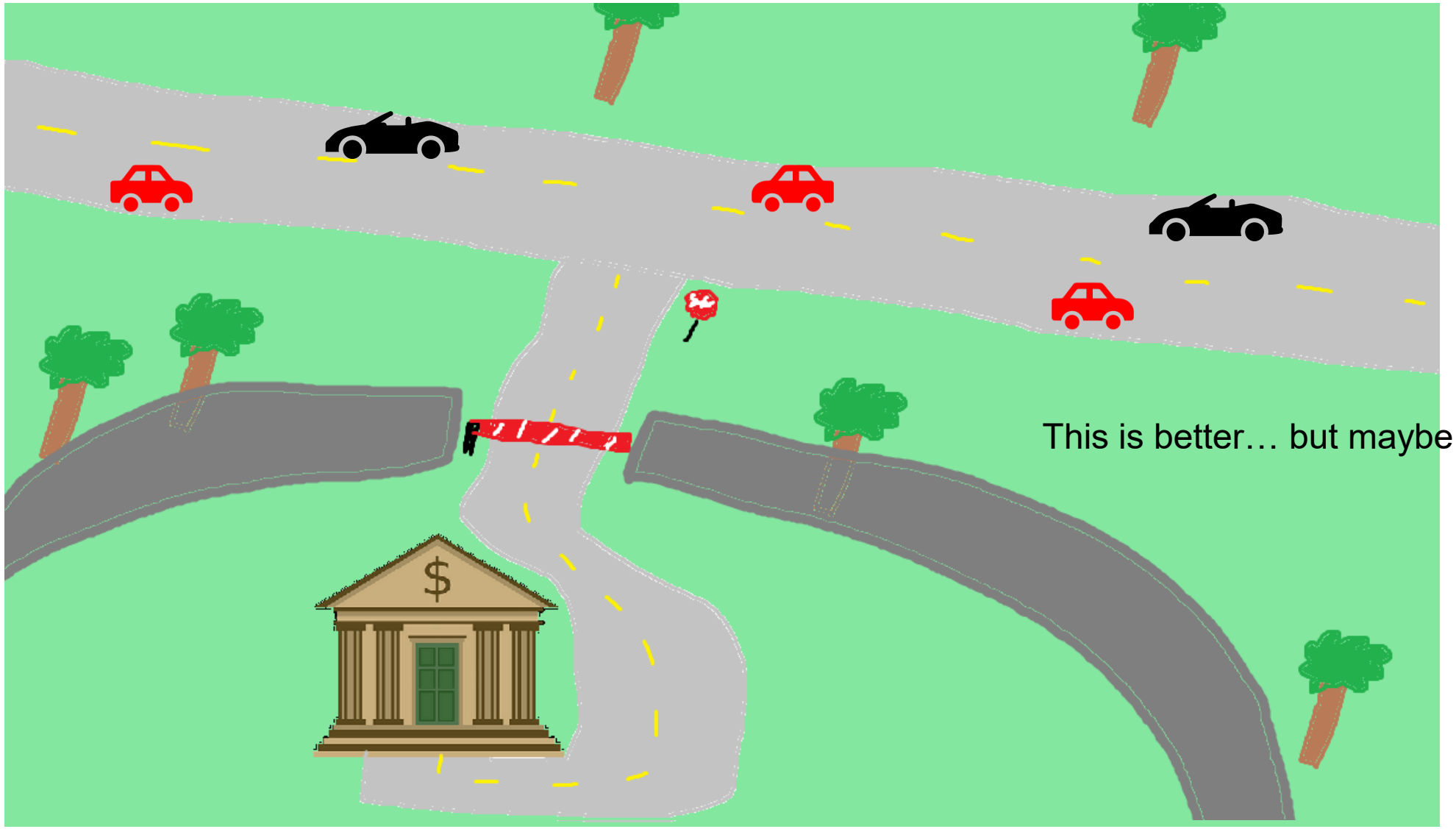
Securing an asset

Securing an asset

A **countermeasure** to this would be to build a wall

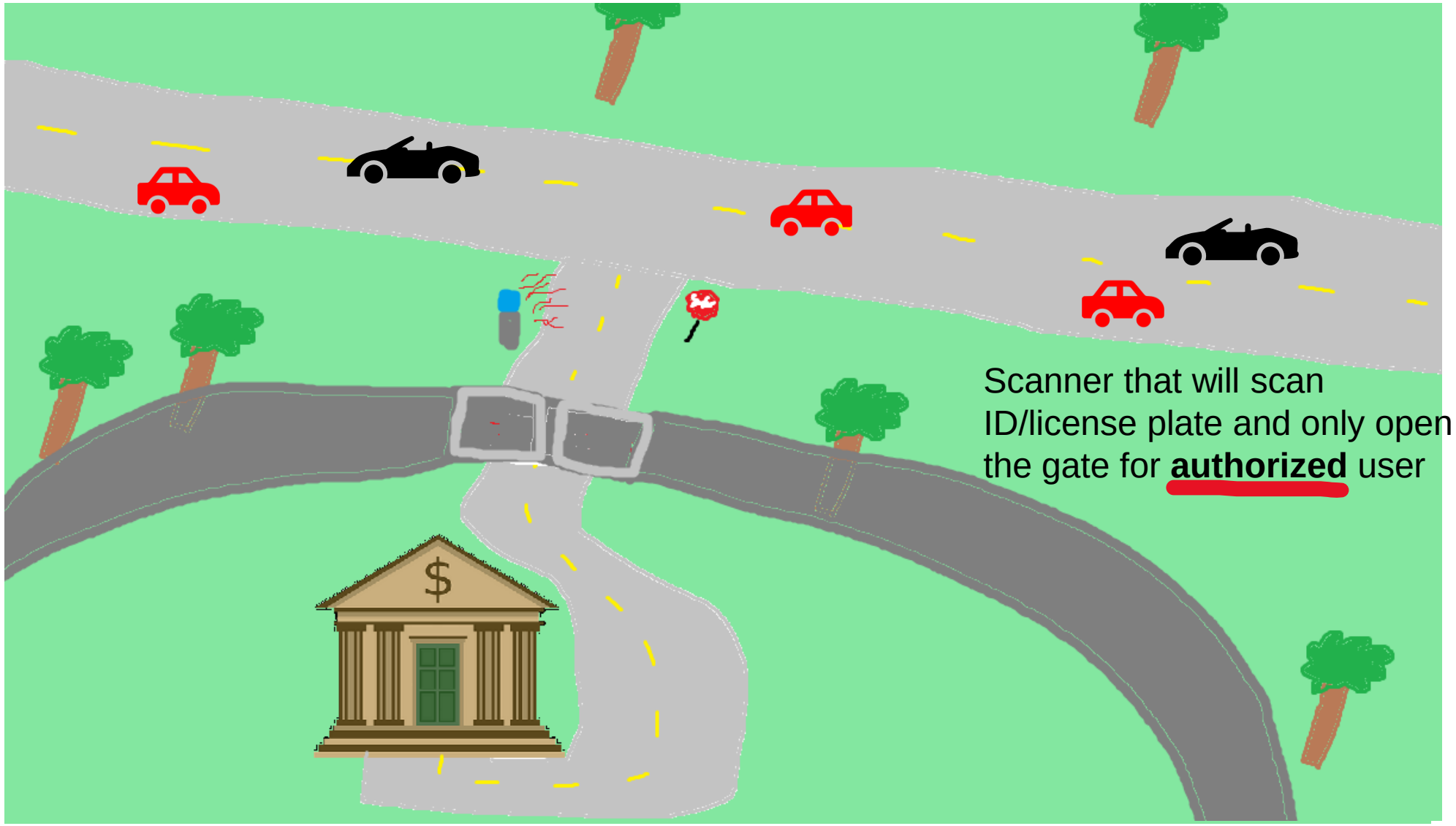


Securing an asset



This is better… but maybe not perfect

Securing an asset

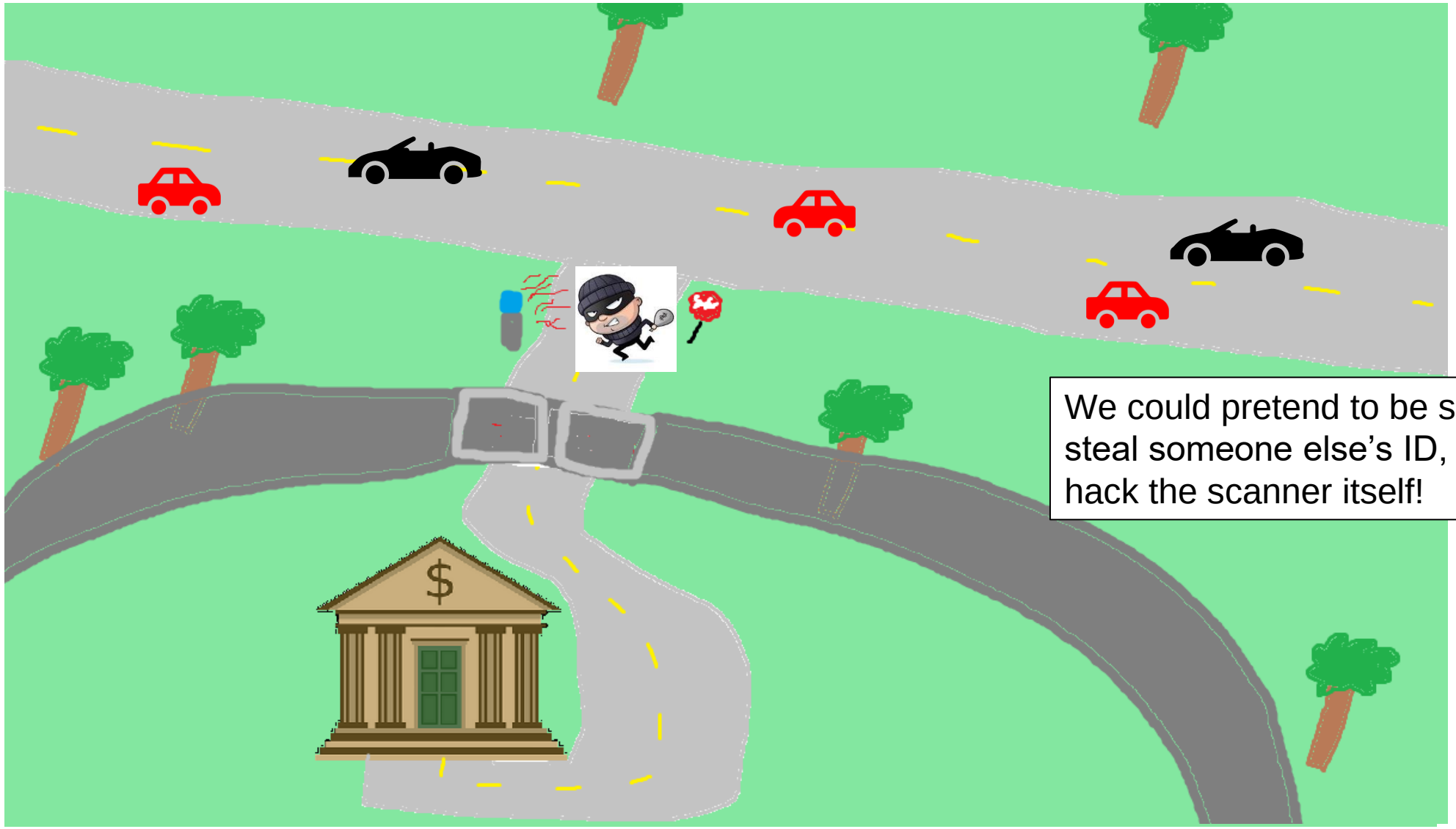


Securing an asset

How do we know they are who they say they are?

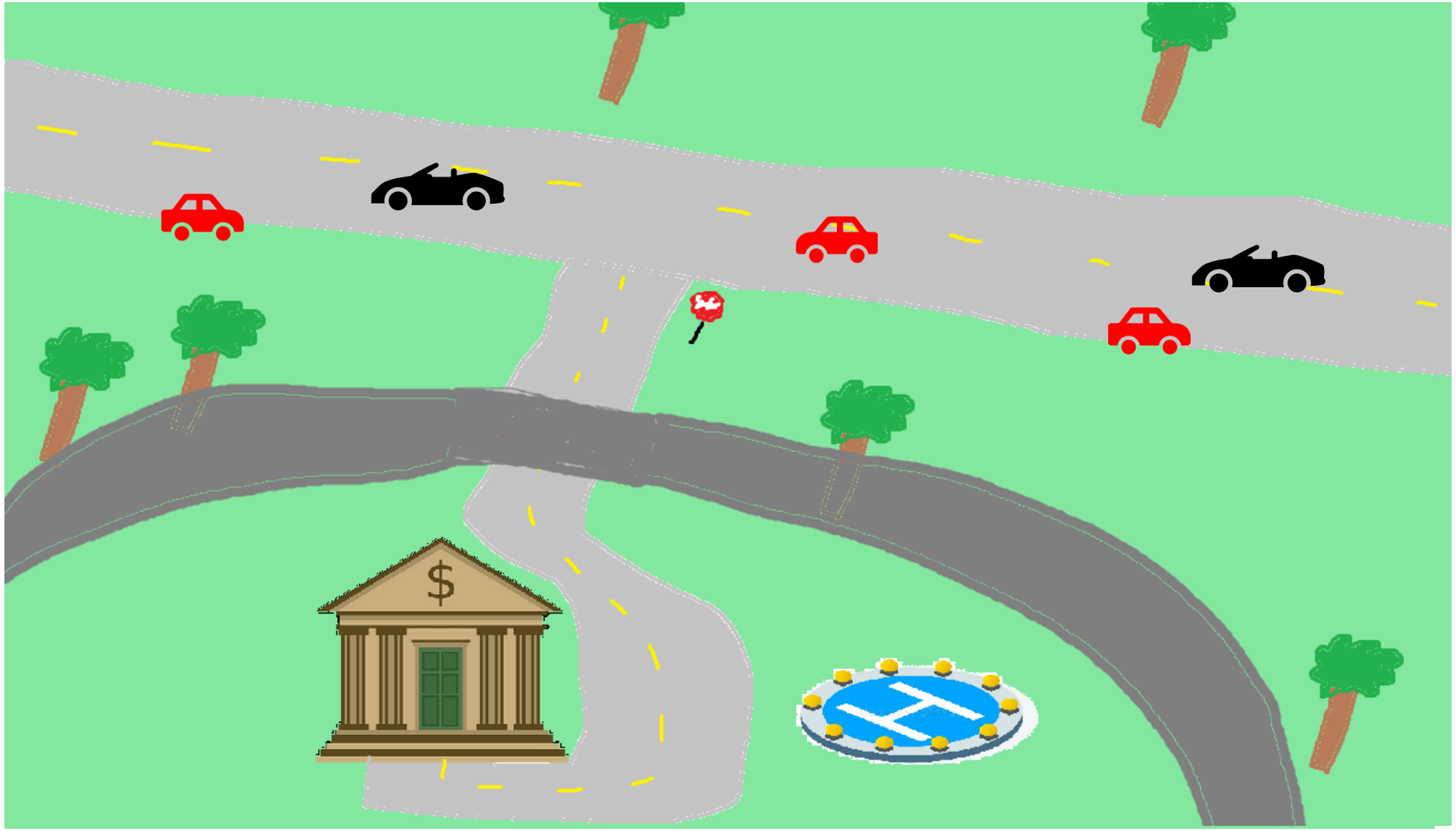
Who can we trust?

Securing an asset



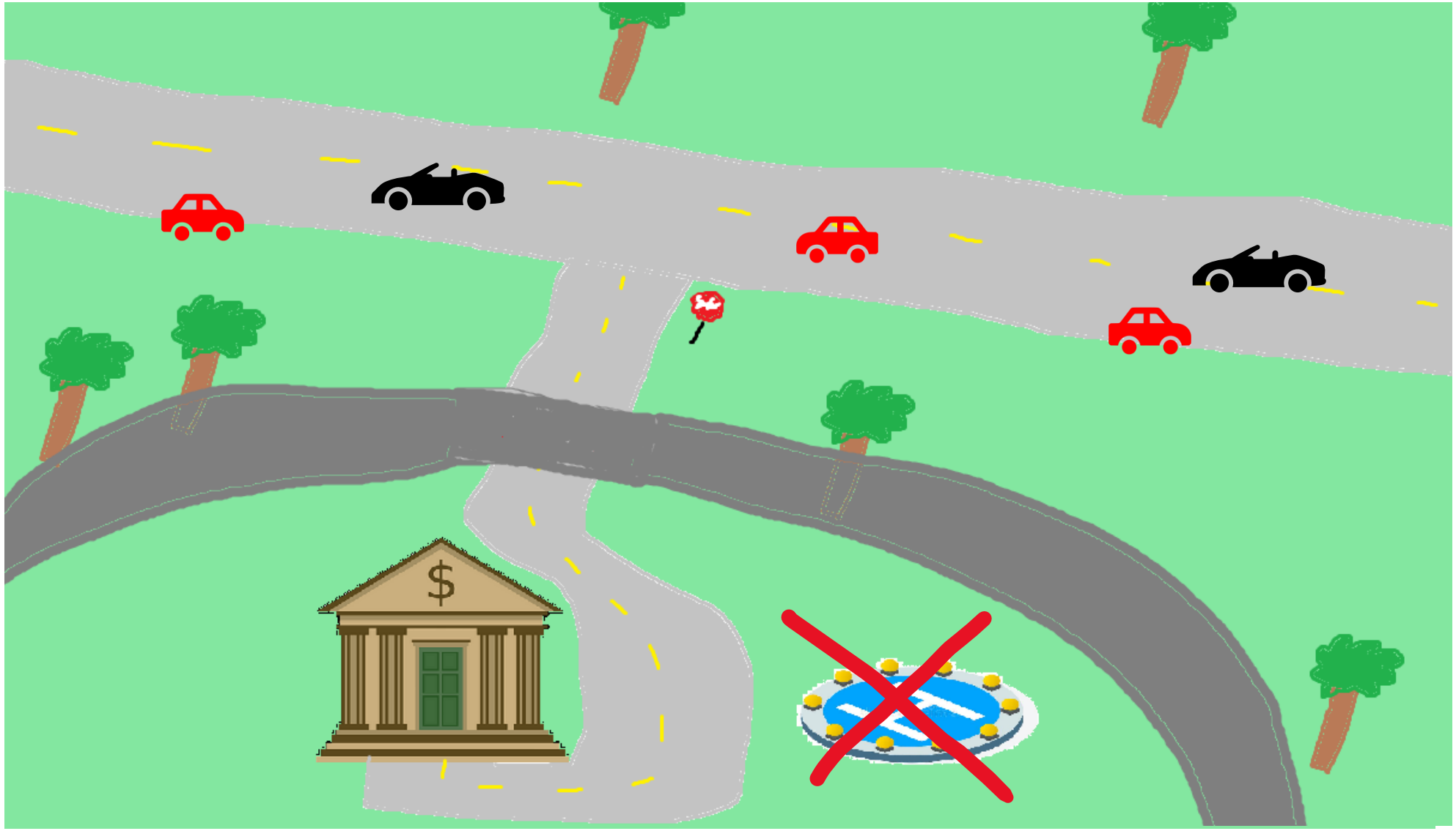
We could pretend to be someone else, steal someone else's ID, or maybe even hack the scanner itself!

Securing an asset



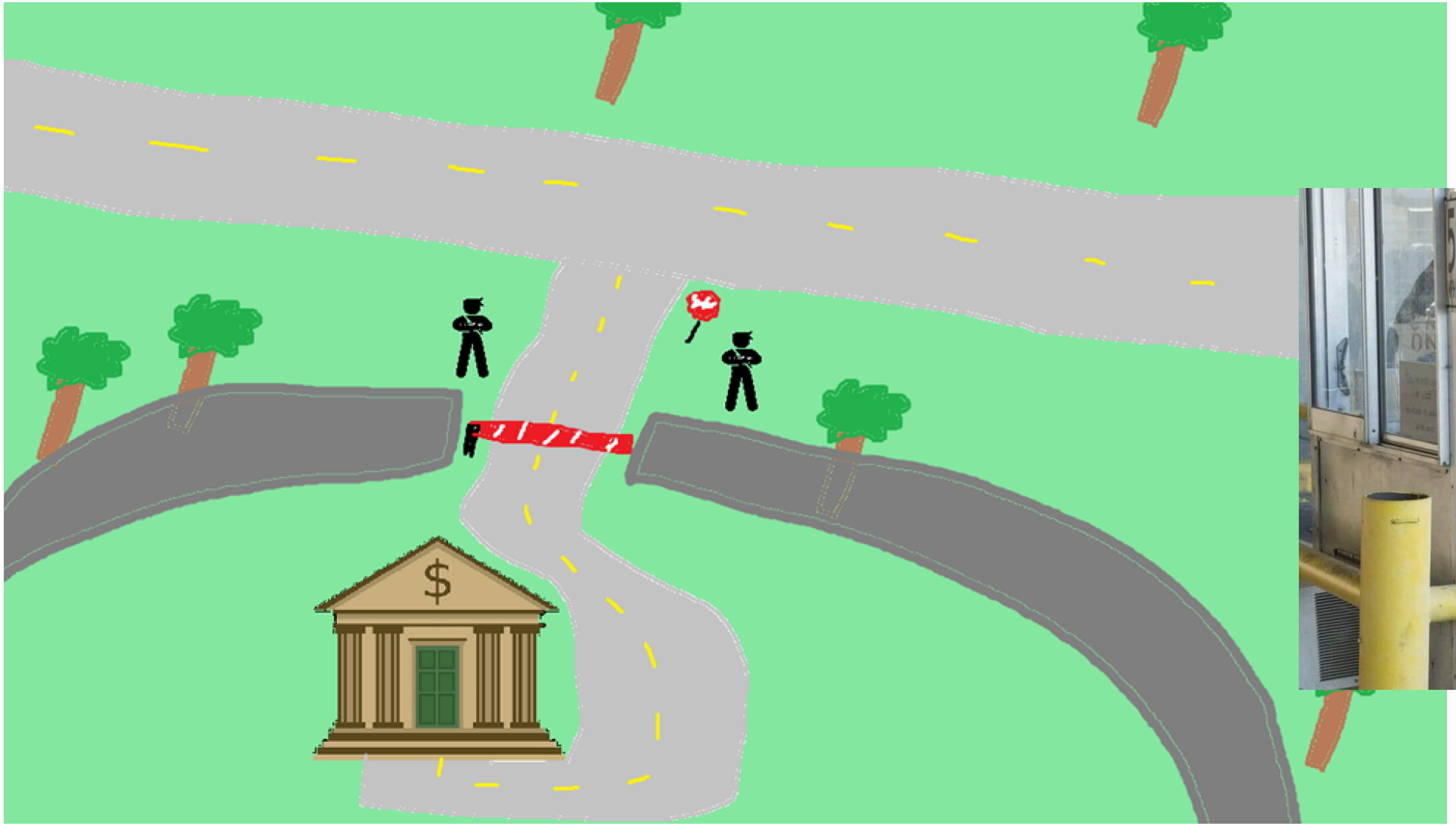
Securing an asset

Security needs to be **accessible** and **useable**



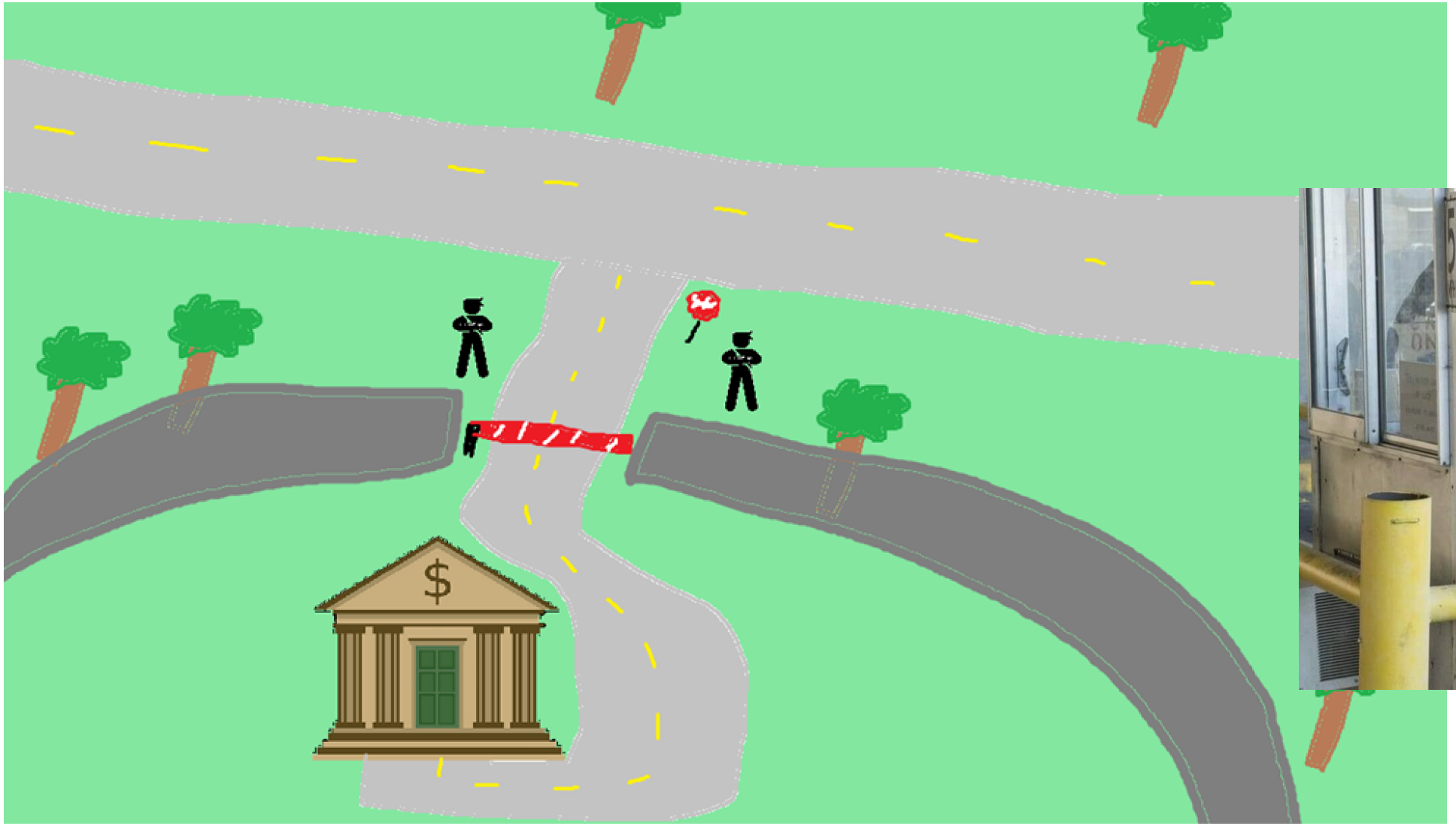
Securing an asset

Let’s add some humans to our design!



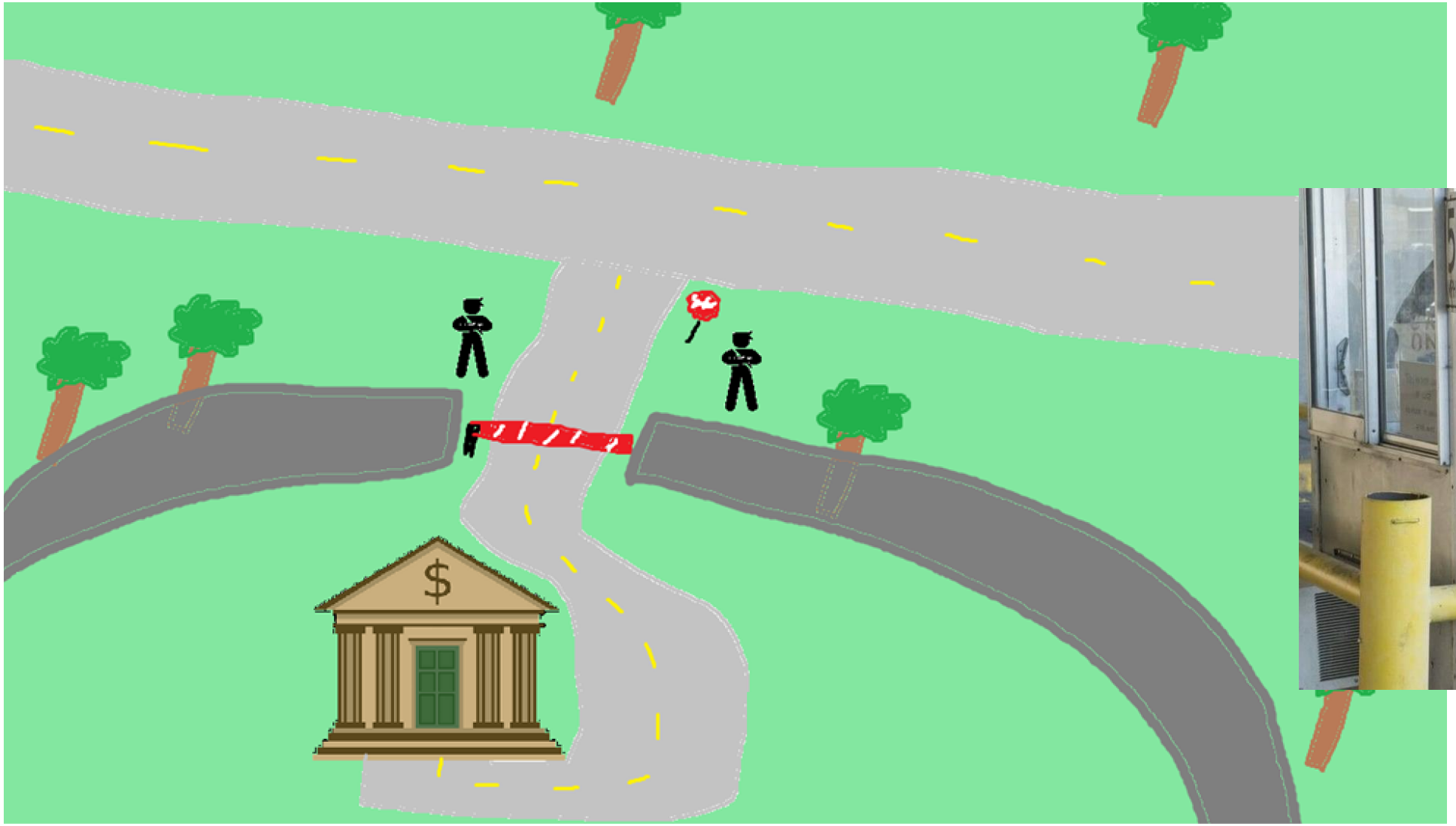
Securing an asset

Consequences of adding humans into our design?



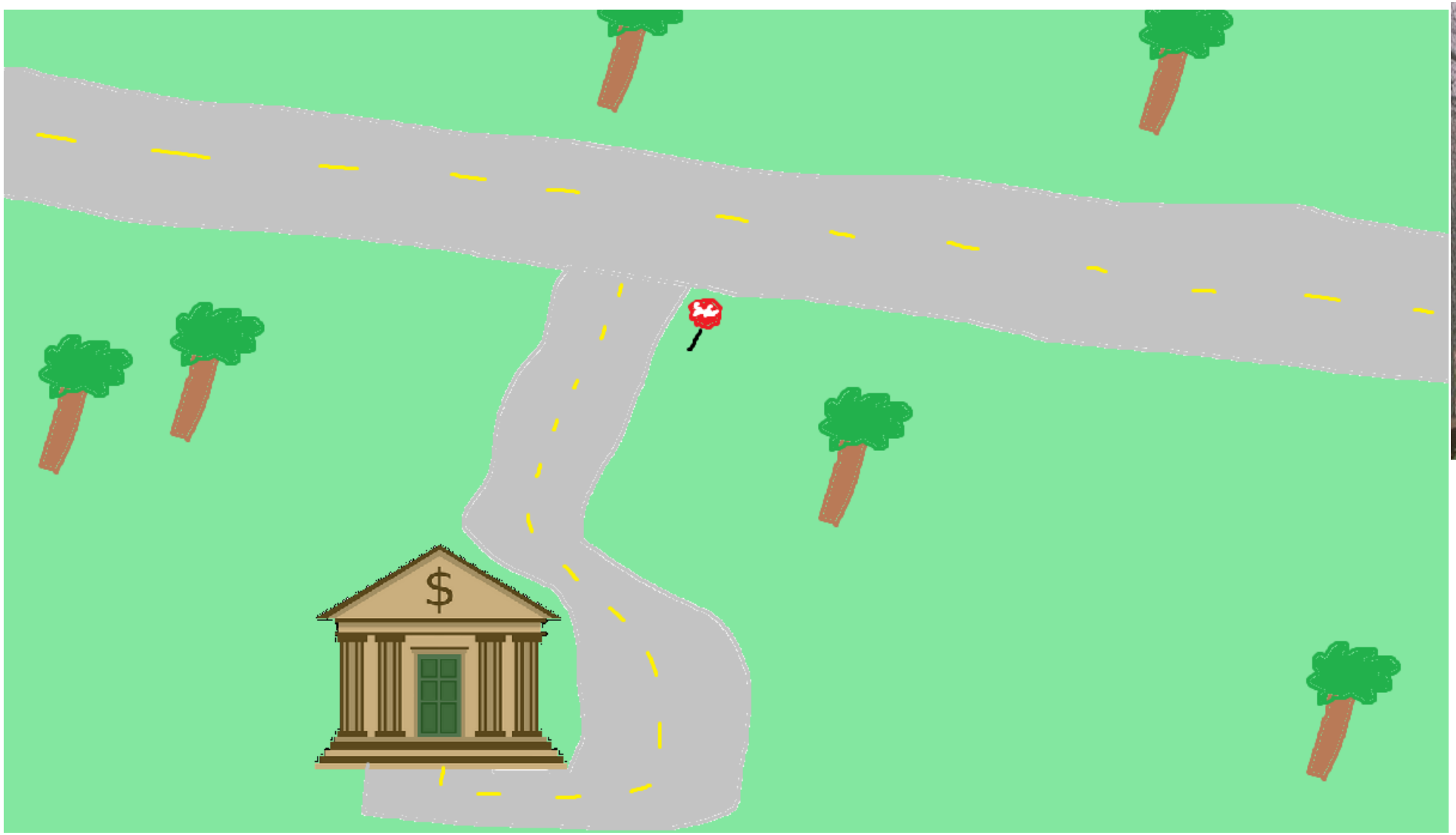
Securing an asset

Humans can be manipulated

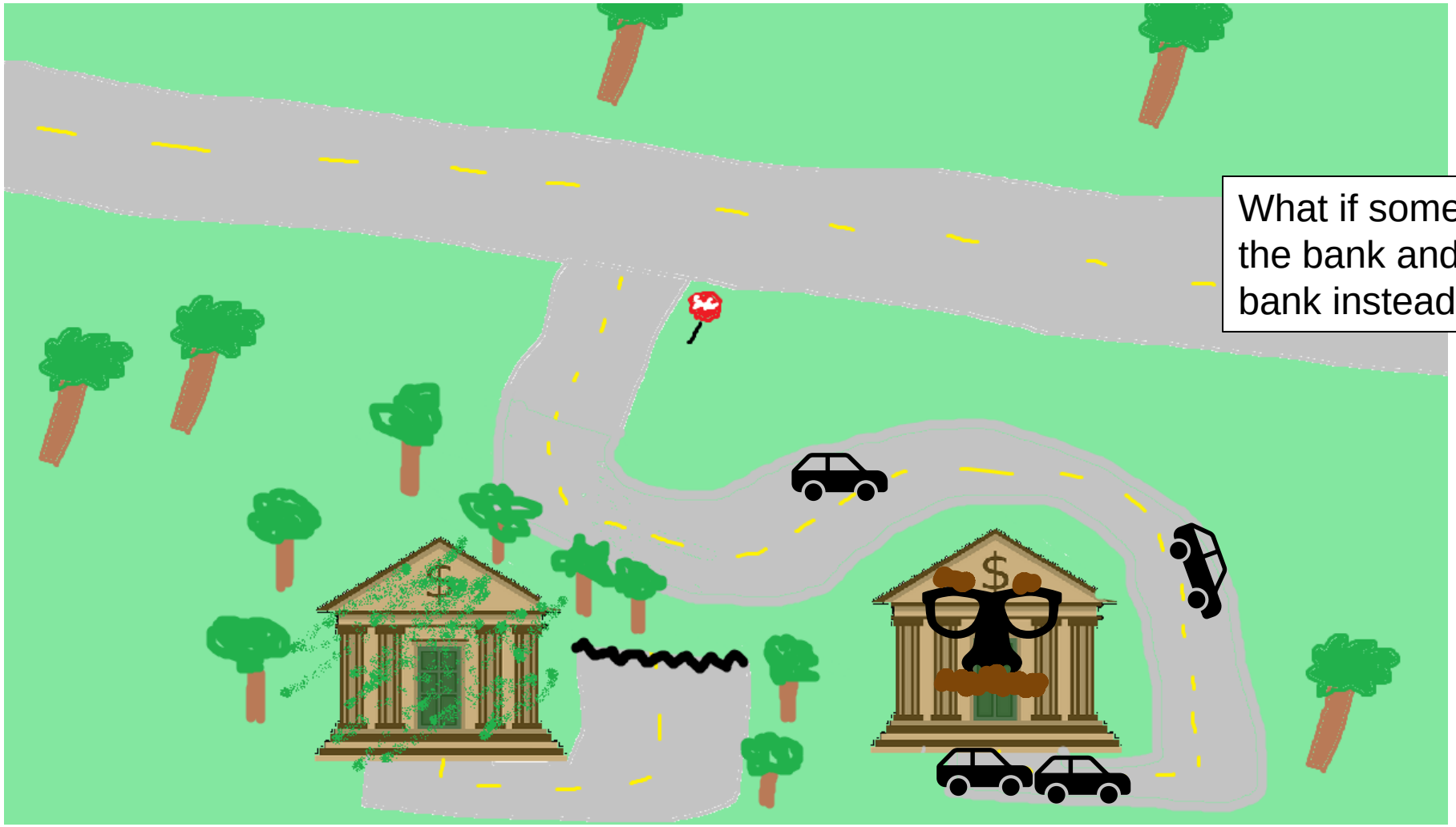


Securing an asset

Oftentimes in security, we must consider even the *craziest* scenarios



Securing an asset



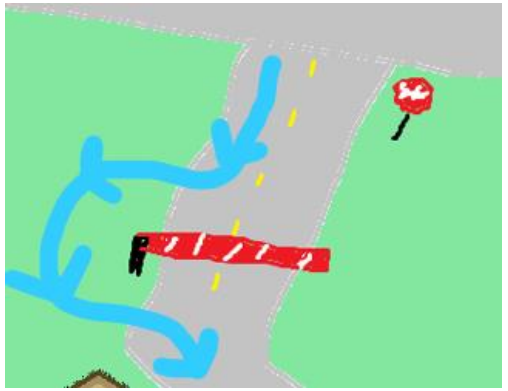
What if someone build an exact replica of the bank and tricks people to go to fake bank instead?

This bank is now controlled by the evil person and can see everything that is happening

CSCI 476 Common Themes

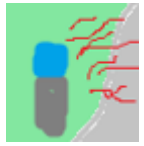
Intended Design of Software

Unpredictability of Humans



Countermeasures

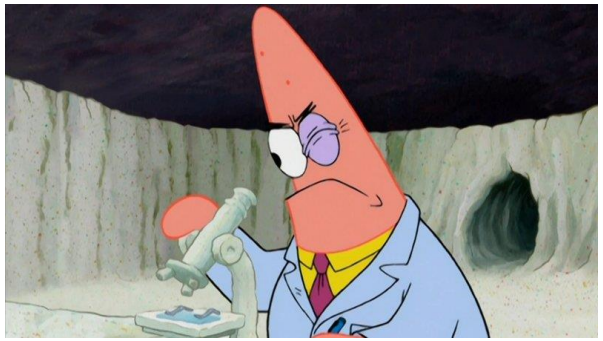
Authorization and **Trust**



Exploitation of powerful tools and programs

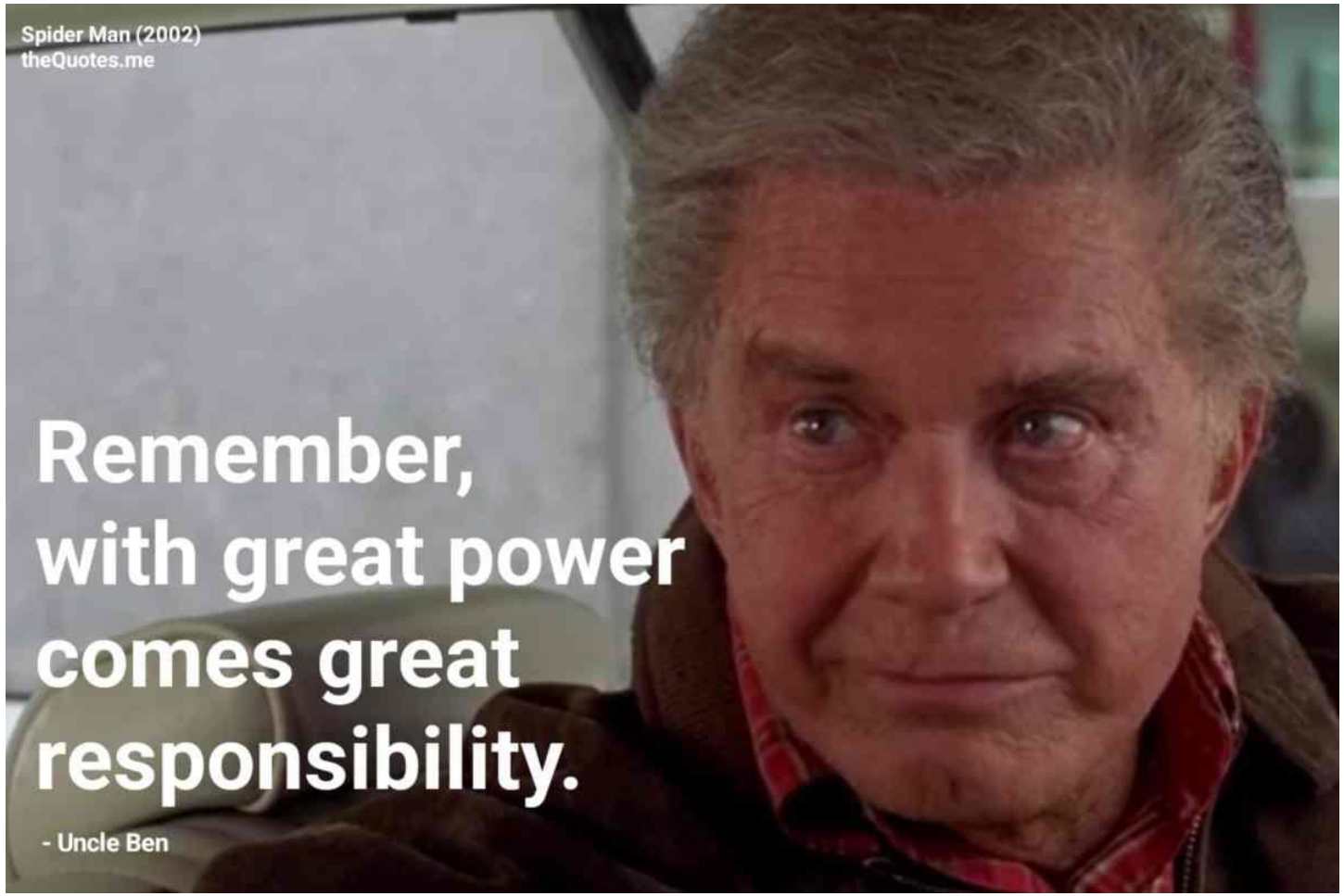
Misdirection and Hijack of control flow

CSCI 476- Course Outcomes



- Understand **important principles of security** and threats to the CIA triad
- Understand a variety of relevant vulnerabilities and defenses in **software** security
- Understand a variety of relevant vulnerabilities and defenses in **network** security
- Understand a variety of relevant vulnerabilities and defenses in **cryptography**
- Given a system, develop a **threat model**, assess potential security weaknesses, and be able to think from the perspective of a threat actor
- Make technical decisions during development of software with security in mind

(I wont be teaching you how to be a hacker…)



You will learn skills that can be used for good and for evil

You should not use tactics learned in this class on real systems

Use your power for good

Reese Pearsall (pierce-all)

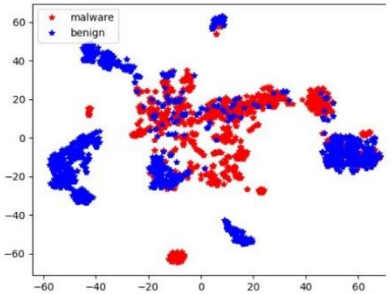
Second year Instructor @MSU
B.S & M.S @ MSU

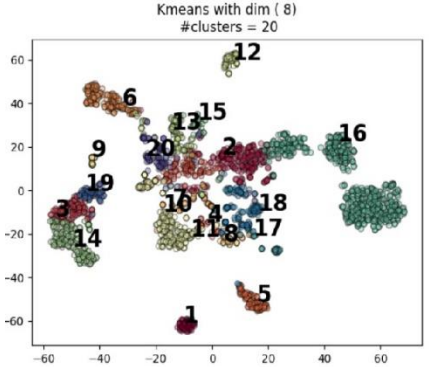
Interests
- Cybersecurity
- Malware analysis and detection
- Cybercrime
- Computer Science Education

Hometown
- Billings, MT

Teaching
- CSCI 132
- CSCI 466
- CSCI 476

Favorite Cereal
- Honey Nut Cheerios





Experience
- Software Engineer and Tester, Techlink (Bozeman)
- Software Engineer, United States Air Force (Hill AFB, Utah)
- Software Engineer, Hoplite Industries (Bozeman)
- Graduate Researcher, MSU (Bozeman)

Outside of academia
- Video games, New England Patriots, Fantasy Football, ~~TikTok~~, Movies, Memes, *The Bachelor*, Naps

Contact

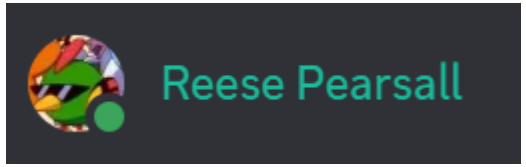
Email: reese.pearsall@montana.edu (I will respond as soon as I can)

Office Hours: Monday, Wednesday, Friday 1:00 – 2:00 PM
Thursday 1:30-2:30PM
and by appointment

I am in my office a lot. If my door is open, you can always come talk to me

Office: Barnard Hall 361

I am also very responsive on Discord! (@reese_p)



Logistics

Class Meetings

TR: 3:05 PM – 4:20
Romney Hall 315

All lectures will be recorded and put on the website

CSCI 476: Computer Security

Fall 2023

Quick Links

-Syllabus

-Project Details

-Github Repo for Class Code

-SEED Labs Information

Date	Topic	Reading	Slides	Assignment
Thursday August 24th	Syllabus and Course Roadmap			Please Fill out the Course Questionnaire!
Tuesday August 29th	Lab setup			
Thursday August 31st	Computer Architecture Review			
Sunday September 3rd				
Tuesday September 5th	Processes and Forking			
Thursday September 7th	Operating Systems in a nutshell			
Sunday September 10th				
Tuesday September 12th	SET UID			
Thursday September 14th	SET UID			
Sunday September 17th				

Course Website: https://www.cs.montana.edu/pearsall/classes/fall2023/476/main.html

We will be using Discord for class communication and for announcements

Get your role and change your nickname!

Prerequisites

- CSCI 232- Data Structures and Algorithms
- ~~CSCI 460- Operating Systems (recommended)~~
- ~~CSCI 466- Networks (recommended)~~
- CSCI 366- Computer Systems (recommended)
- CSCI 112- Programming in C (HIGHLY HIGHLY HIGHLY recommended)

Prerequisites

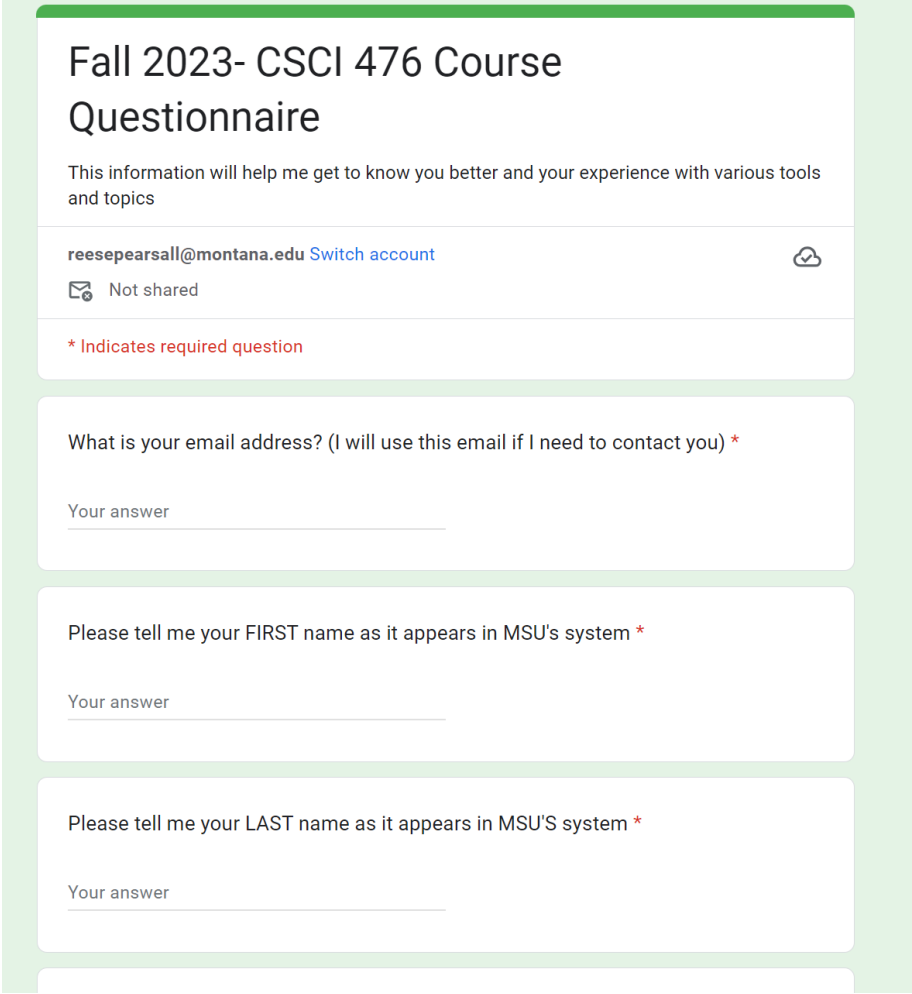
- CSCI 232- Data Structures and Algorithms
- CSCI 366- Computer Systems (recommended)
- CSCI 112- Programming in C (HIGHLY HIGHLY HIGHLY recommended)

Before taking this class, I expect you to be comfortable with

- Basic Python and C programming
- Basic Linux command line navigation
- Basic computer architecture (Memory, CPU, Assembly, Hex, OS, etc) we will review this

Schedule

Course Questionnaire



Fall 2023- CSCI 476 Course Questionnaire

This information will help me get to know you better and your experience with various tools and topics

reesepearsall@montana.edu Switch account

Not shared

* Indicates required question

What is your email address? (I will use this email if I need to contact you) *

Your answer

Please tell me your FIRST name as it appears in MSU's system *

Your answer

Please tell me your LAST name as it appears in MSU'S system *

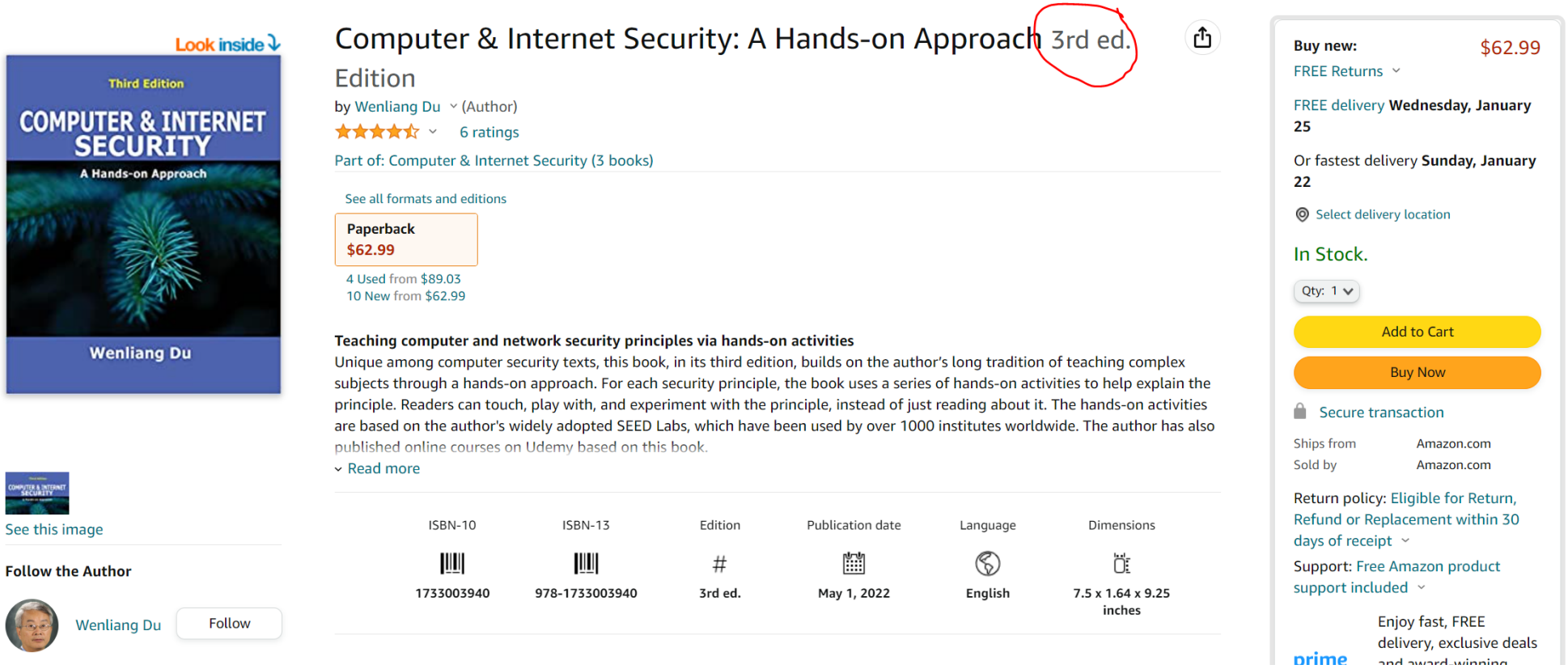
Your answer

Please take some time to do the course questionnaire today or tomorrow

Your answers are important to me and will help make this class a better experience

Part of your grade for Lab 0 will be for completing the questionnaire

Textbook



- I will not require you to get the textbook, but it is a great resource for learning the material and doing the assignments

SEED Labs

The majority of work for this class will be done on the SEED Labs virtual machine

On Tuesday we will walk through the installation process together

It will be helpful if you download this file **before** class on Tuesday.

Ubuntu 20.04 VM

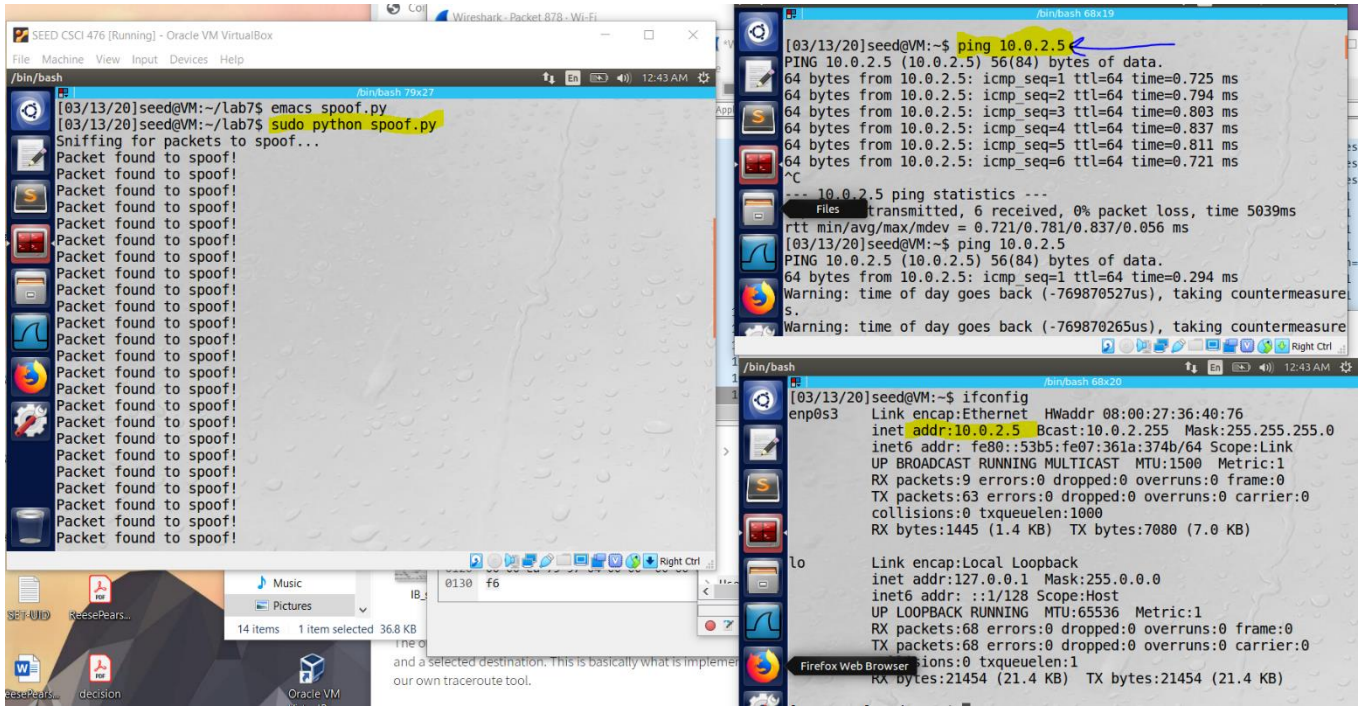
If you prefer to create a SEED VM on your local computers, there are two ways to do that: (1) use a pre-built SEED VM; (2) create a SEED VM from scratch.

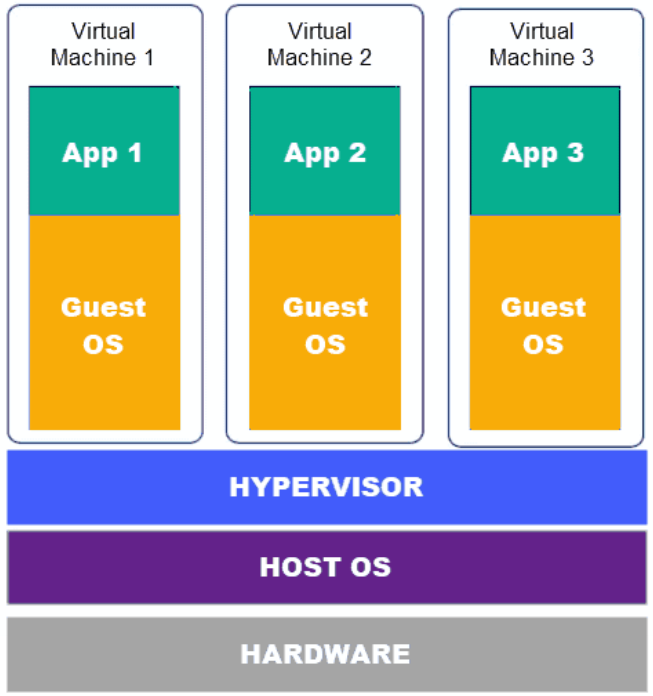
Approach 1: Use a pre-built SEED VM. We provide a pre-built SEED Ubuntu 20.04 VirtualBox image (`SEED-Ubuntu20.04.zip`, size: 4.0 GB), which can be downloaded from the following links.

- Google Drive
- DigitalOcean
- MD5 value: f3d2227c92219265679400064a0a1287
- VM Manual: follow this manual to install the VM on your computer

Approach 2: Build a SEED VM from scratch. The procedure to build the SEED VM used in Approach 1 is fully documented, and the code is open source. If you want to build your own SEED Ubuntu VM from scratch, you can use the following manual.

- How to build a SEED VM from scratch





Grading

- 70% Labs (11 or 12)
- 15% Research Project
- 15% Final Exam

Grading

- **70% Labs** (11 or 12)

➢ Learn by doing, which will enhance your understanding of computer security

➢ We will use the VM to replicate the attacks we discuss in lecture

➢ Follow the instructions, and record your observations and output

➢ Submitted to D2L as a PDF

Grading

- **15% Research Project**

➢ You will explore a cybersecurity-related topic of your choice (one we did *not* discuss in class)

➢ You will have a choice of writing a paper *or* creating a video presentation on the topic

➢ You can submit it at any point in the semester, but deadline is April 23rd

➢ You must get your topic approved by Reese first

Grading

- **15% Final Exam**

➢ Cumulative exam that covers content from the entire semester

➢ Exam consists of short answer questions

➢ Will take place during finals week (in-person)

Late Assignment Policy

Late Assignment Policy

You will be given 1 virtual late passes. Late passes allow you to submit a lab up to 48 hours late with NO penalty-- no excuse required.

To use a late pass, you must indicate in your submission that you are electing to use a late pass (e.g. at the top of your lab report and in the comment box on your submission in D2L).

Note that you cannot change this decision later.

If you do not use a late pass, the penalties for late submissions are as follows:

- < 24 hours: 25%
- < 48 Hours 50%
- > 48 hours: no credit.

Grading Scale

- 93+: A
- 90+: A-
- 87+: B+
- 83+: B
- 80+: B-
- 77+: C+
- 73+: C
- 70+: C-
- 67+: D+
- 63: D
- 60: D-

At the end of the semester, if you are within 1% of the next letter grade, I will bump you up

I will not curve exams or final grades unless it is needed

Plagiarism and Academic Misconduct

Plagiarism and cheating is very not cool

Plagiarism and Academic Misconduct

Plagiarism and cheating is very not cool

You are **not** allowed to submit something that is not your own, and you are not allowed to steal solutions from other groups and modify it

(Generally, I am ok with students sharing ideas and working on their separate solutions together)

I have a Chegg and Course Hero membership. **Don't do it**

Using small snippets of code from the internet is acceptable, but you should leave a reference in the comments

MSU Resources

- Diversity
- Counseling
- Disabilities

How to do well in this class

- **Get started on labs early**
- Get help when you need it
- Come to class and office hours

How to do well in this class

- **Get started on labs early**
- Get help when you need it
- Come to class and office hours

- **Try to have fun**

Questions?