CSCI 476: Computer Security

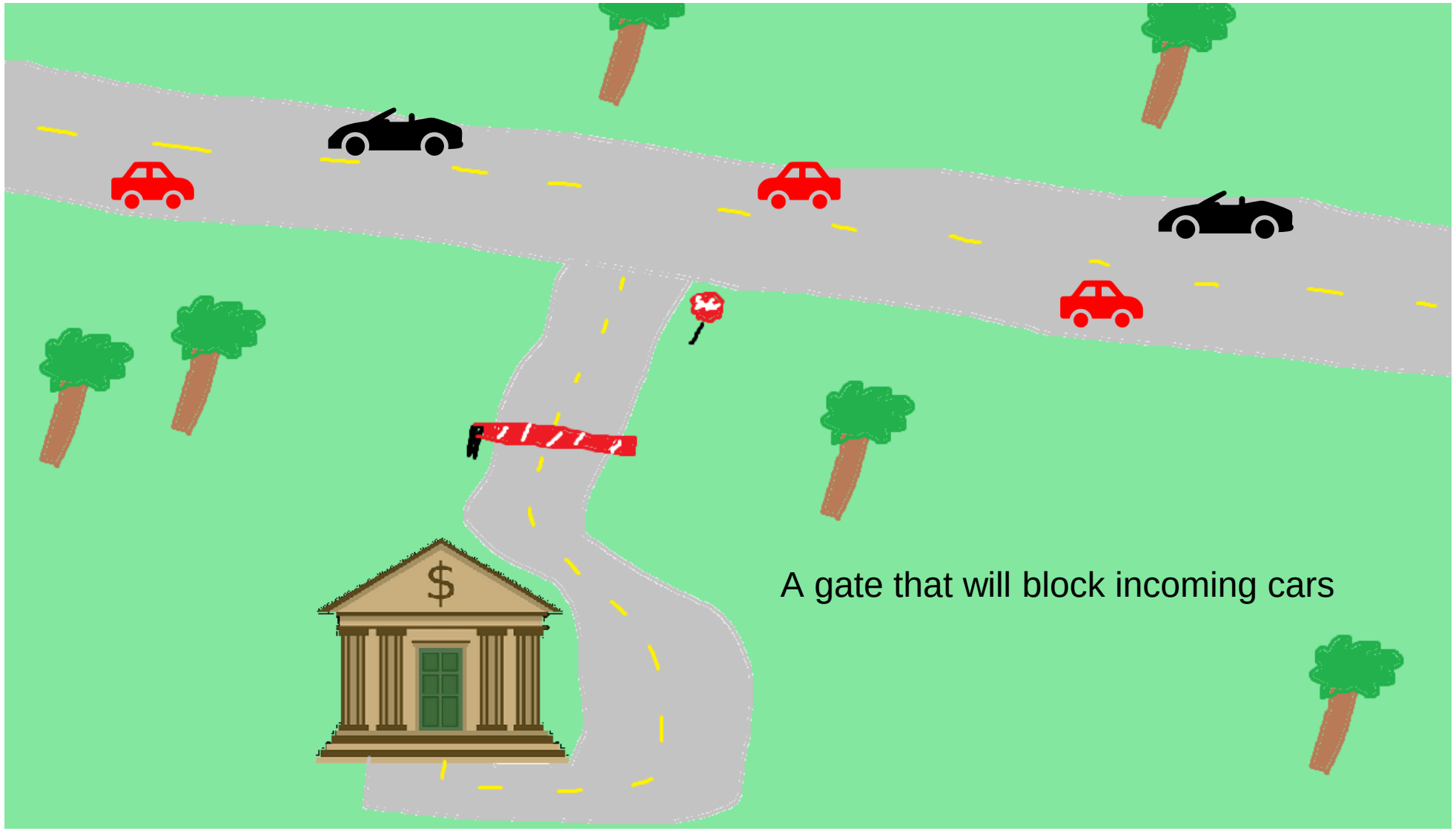
Introduction, Syllabus, and Logistics

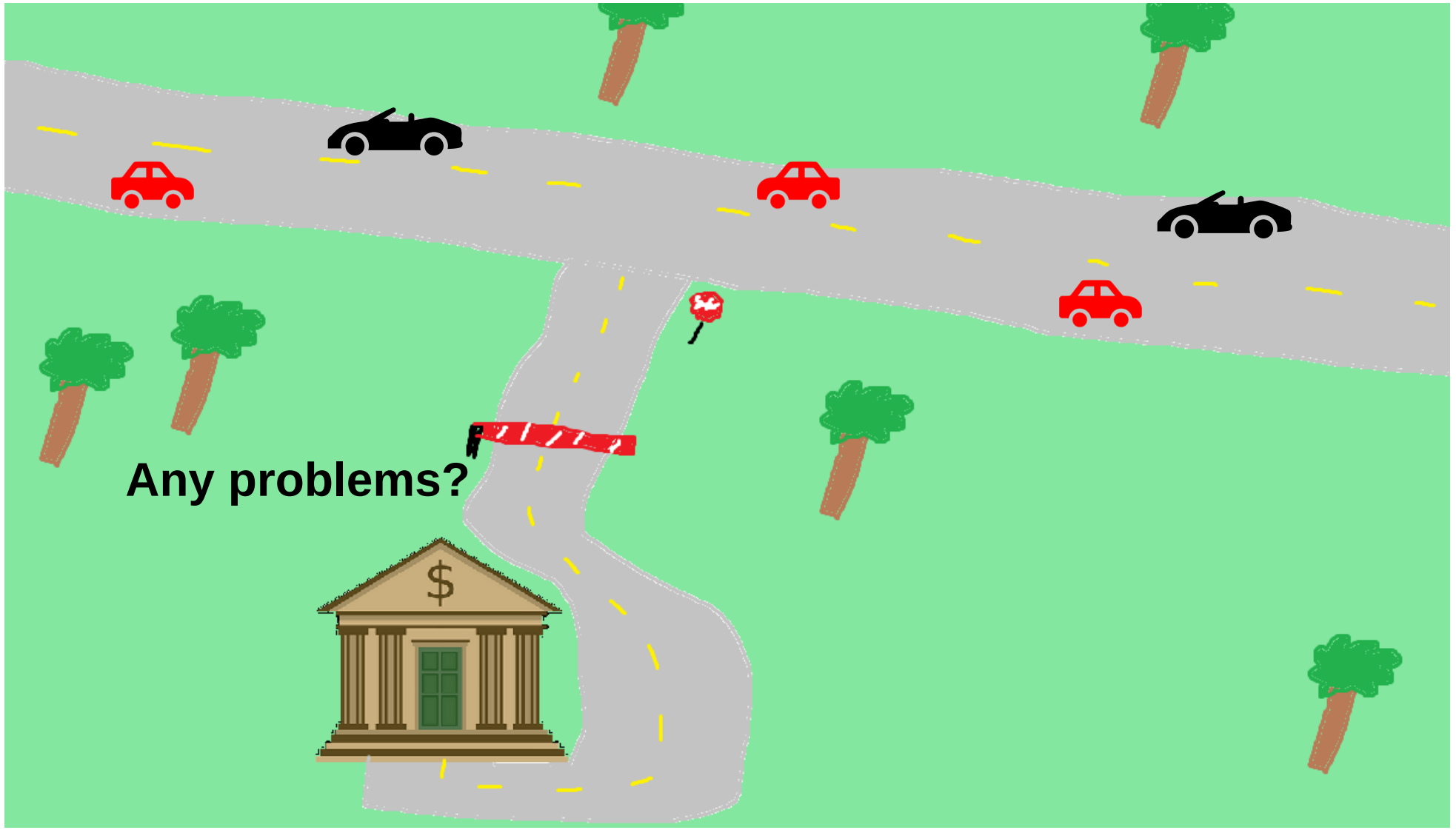
Reese Pearsall

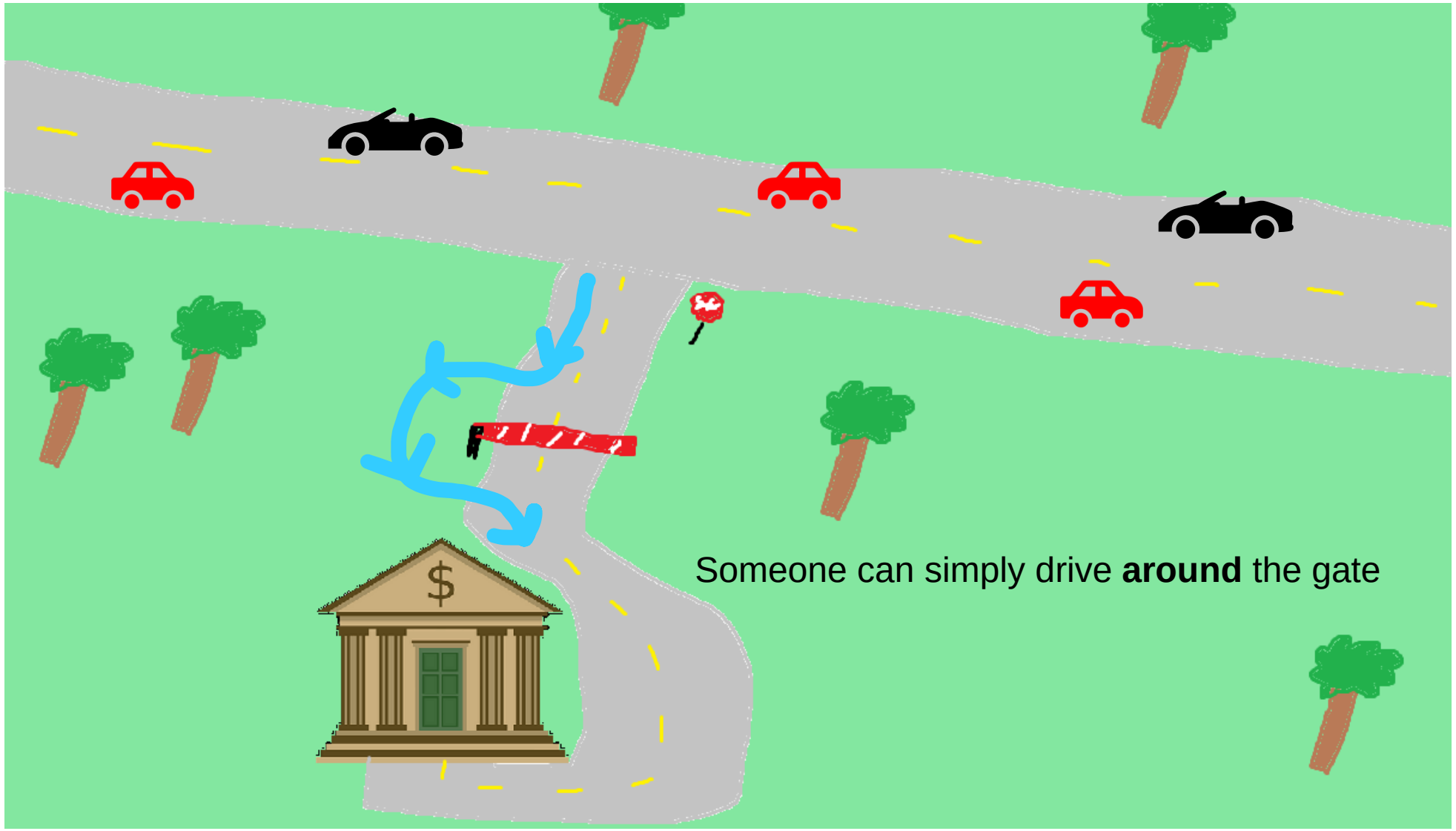
Fall 2024

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


We need to secure the area around the bank
Only people that are allowed should be able to pass into the bank


$
A gate that will block incoming cars

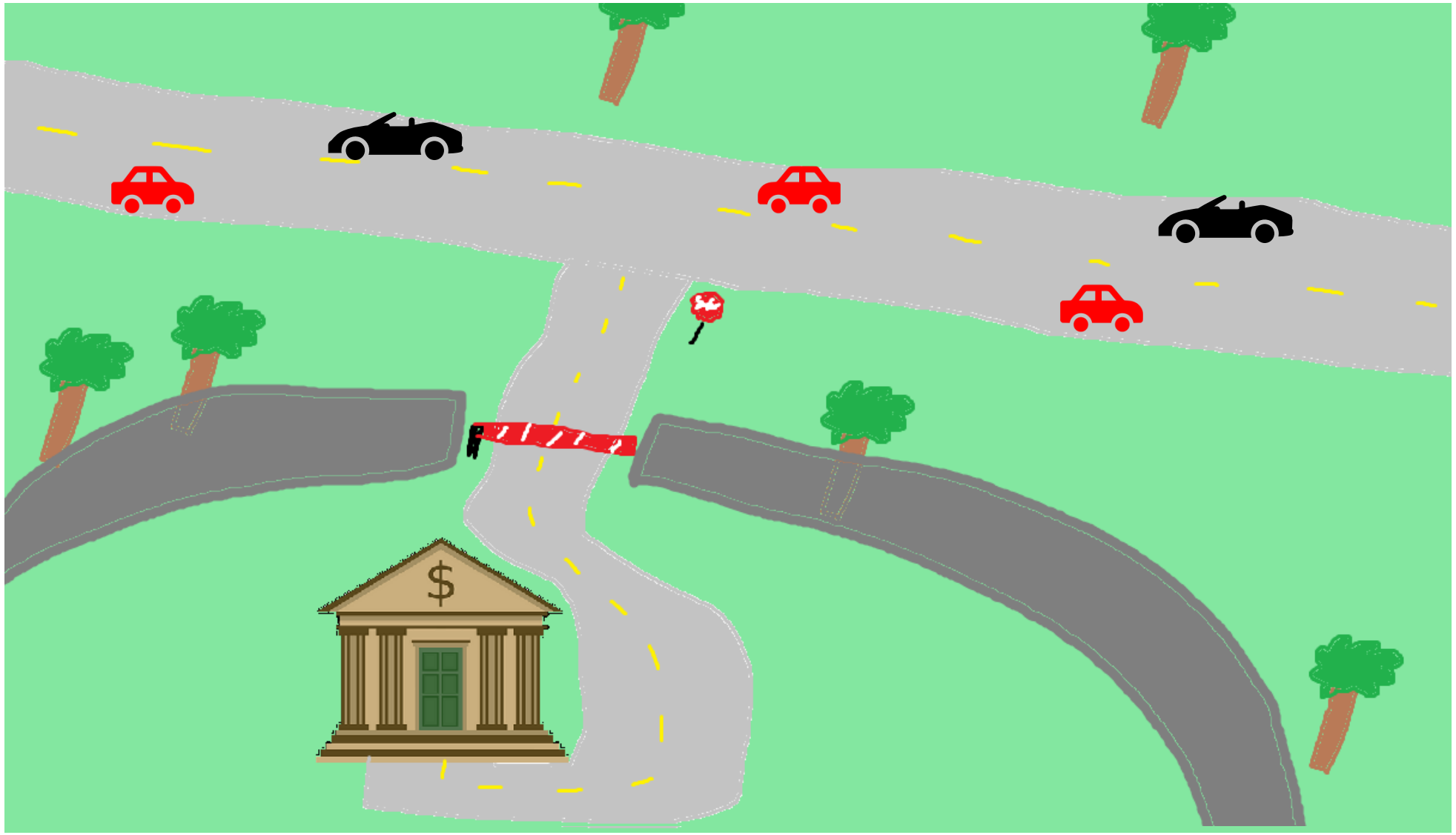

Any problems?
$

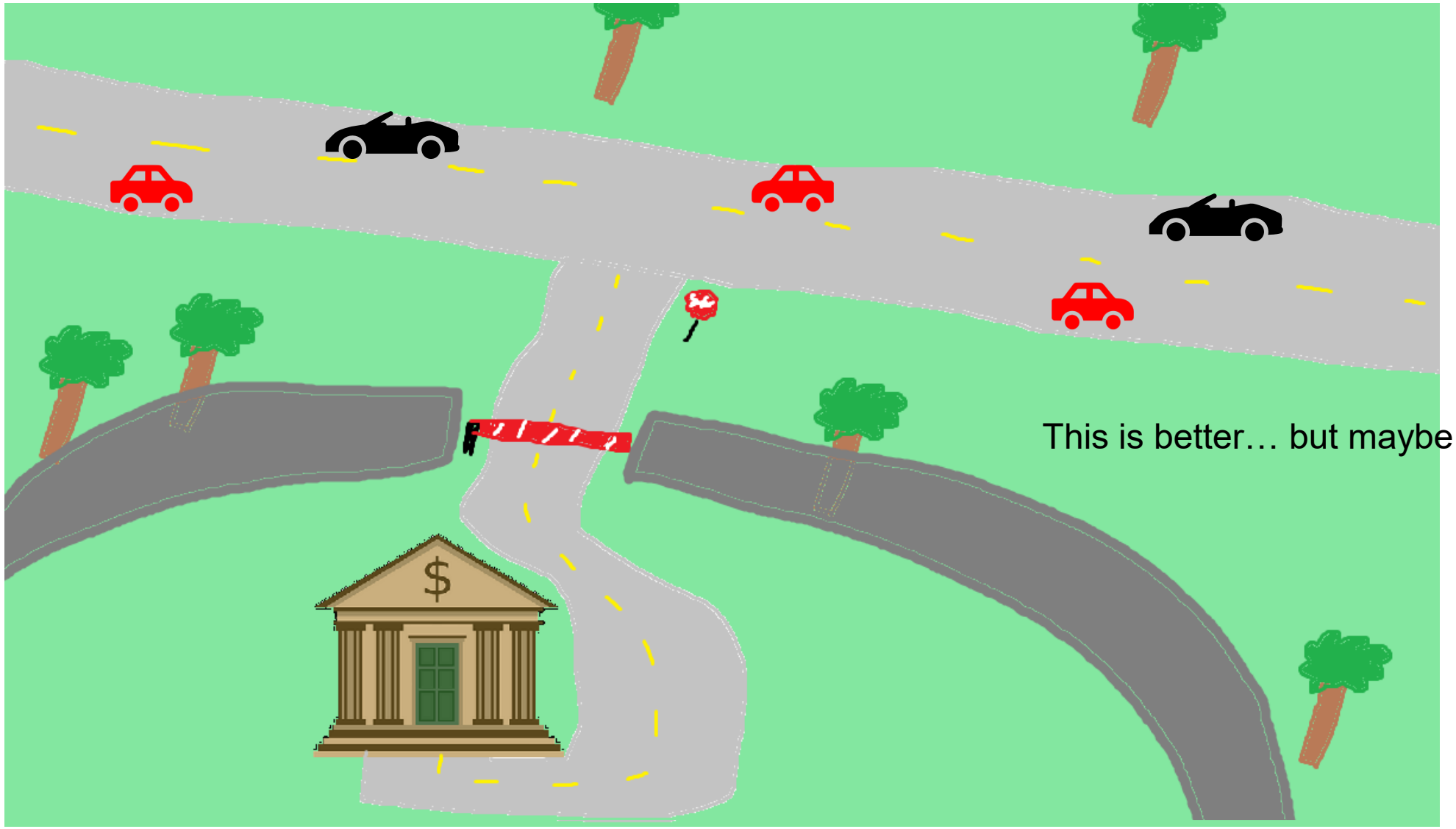

$
Someone can simply drive **around** the gate


They don’t even need to use a road!

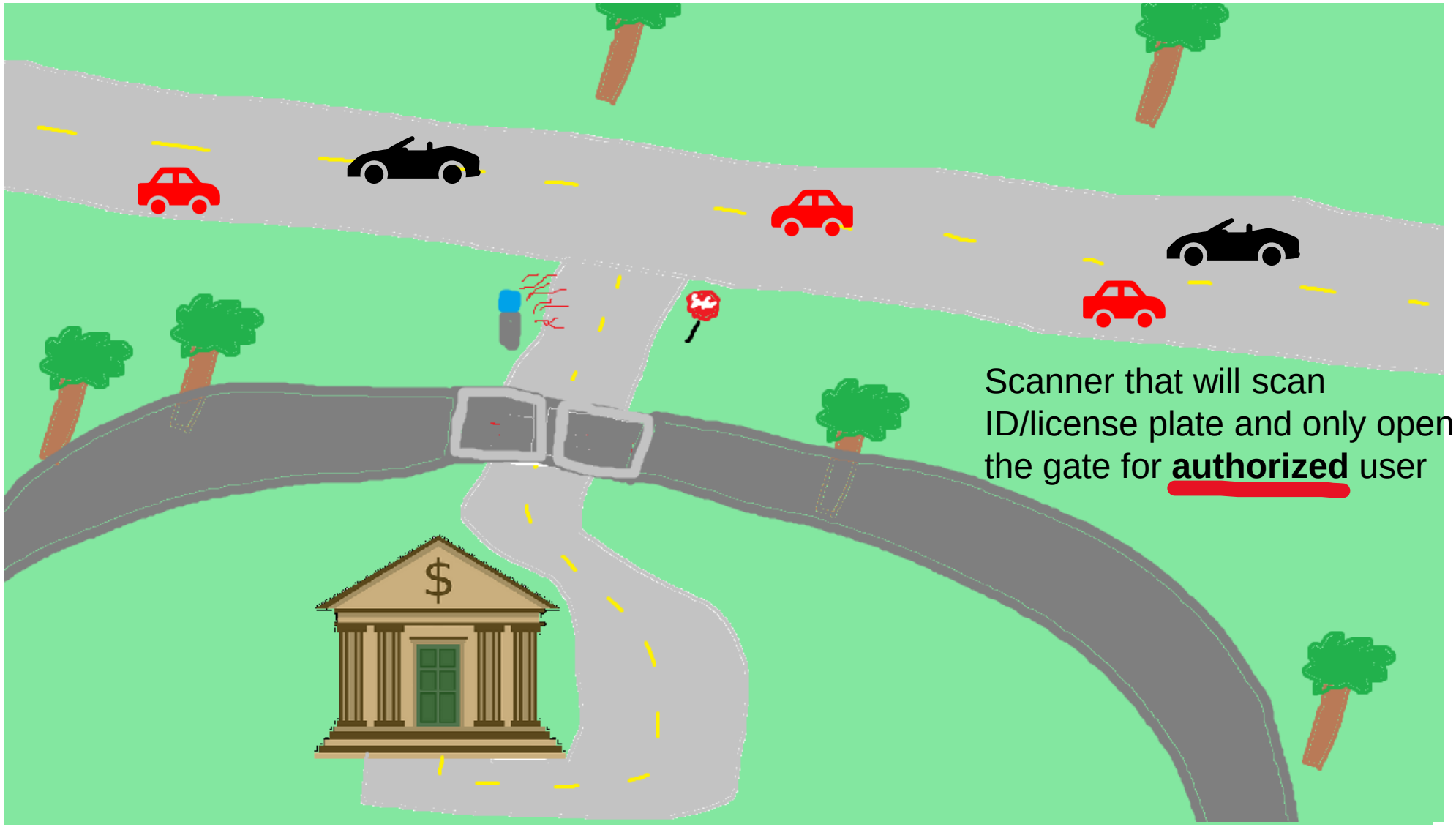

to use a road!

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



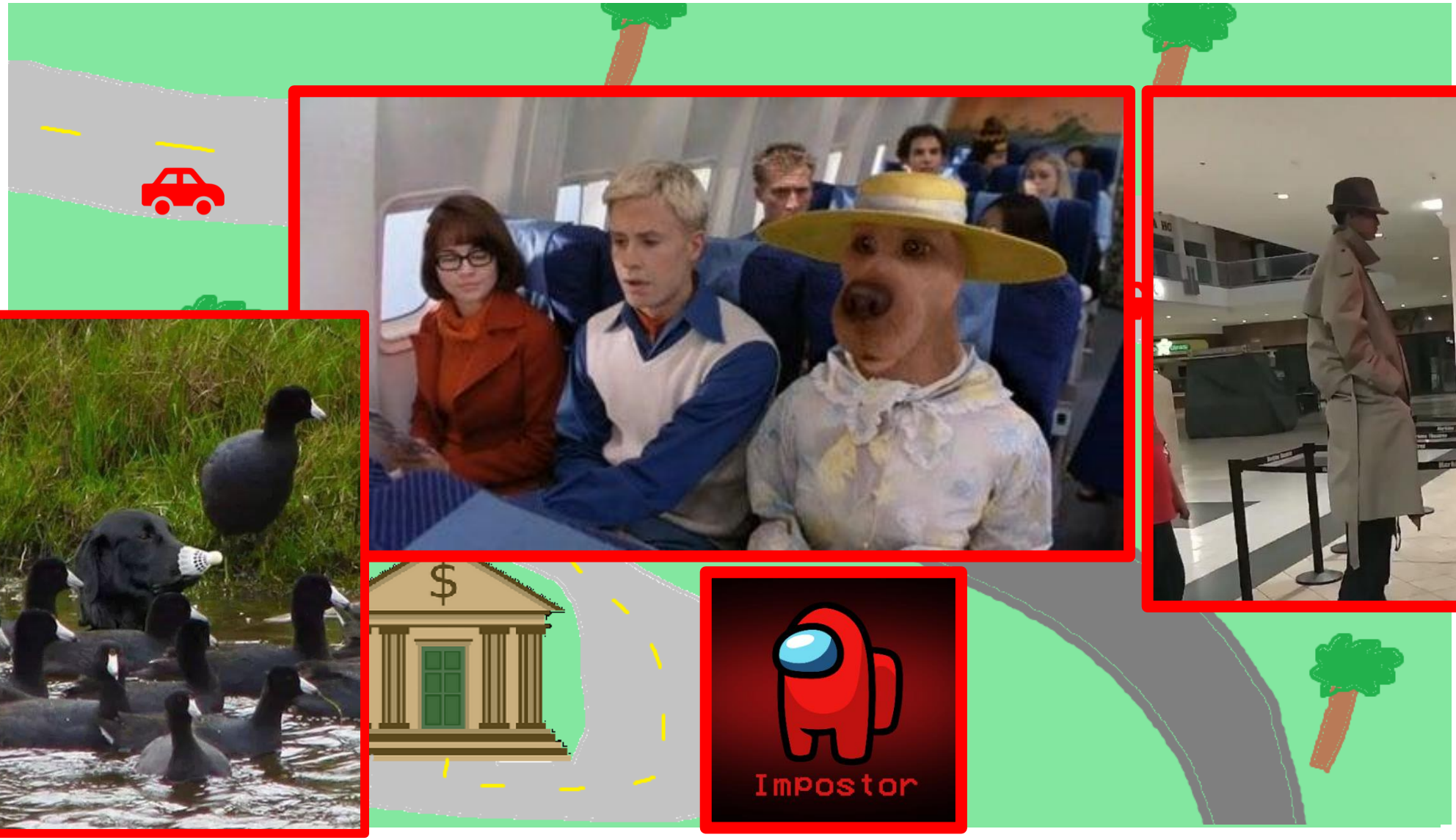


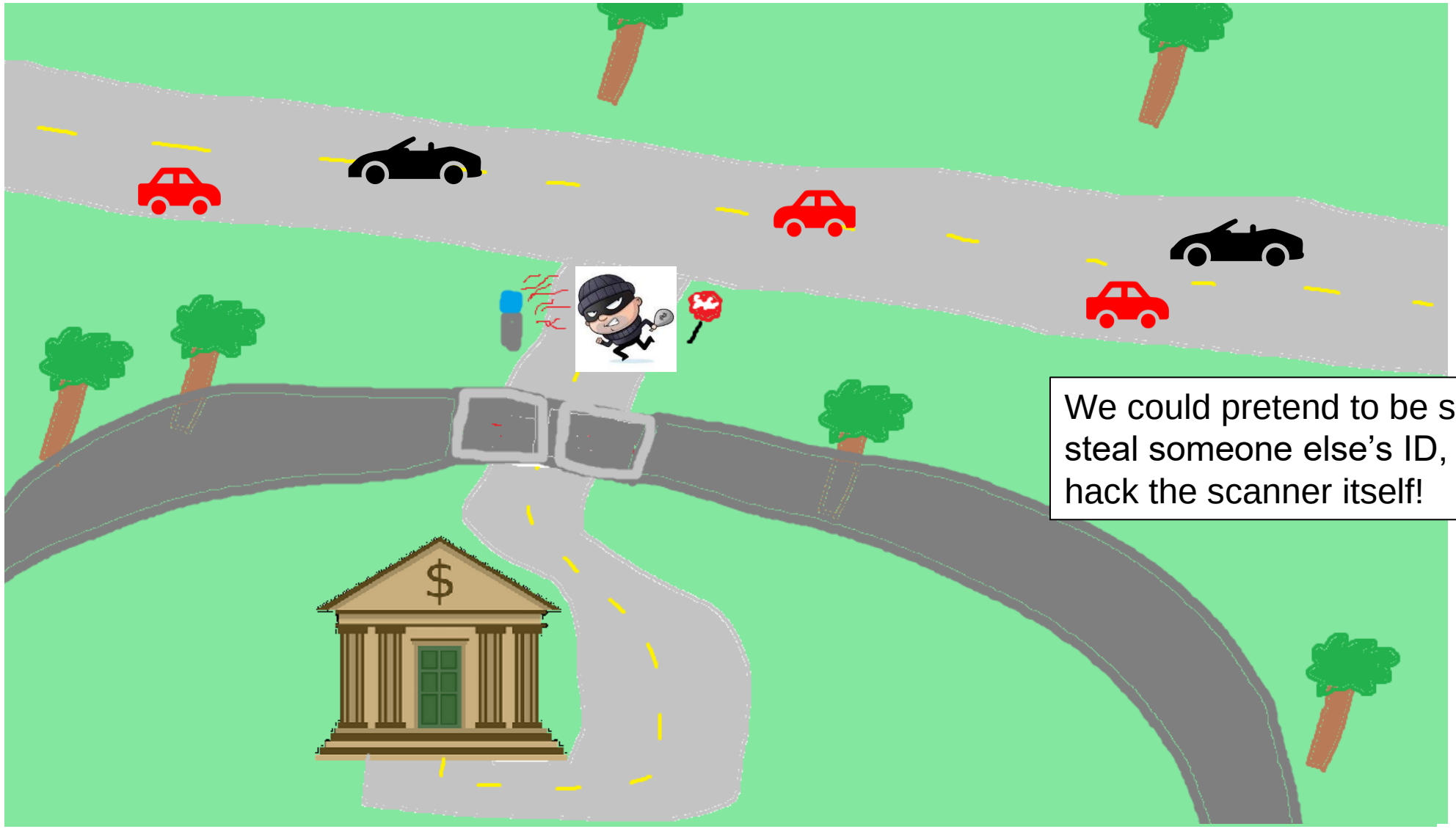
This is better… but maybe not perfect


Scanner that will scan ID/license plate and only open the gate for **authorized** user

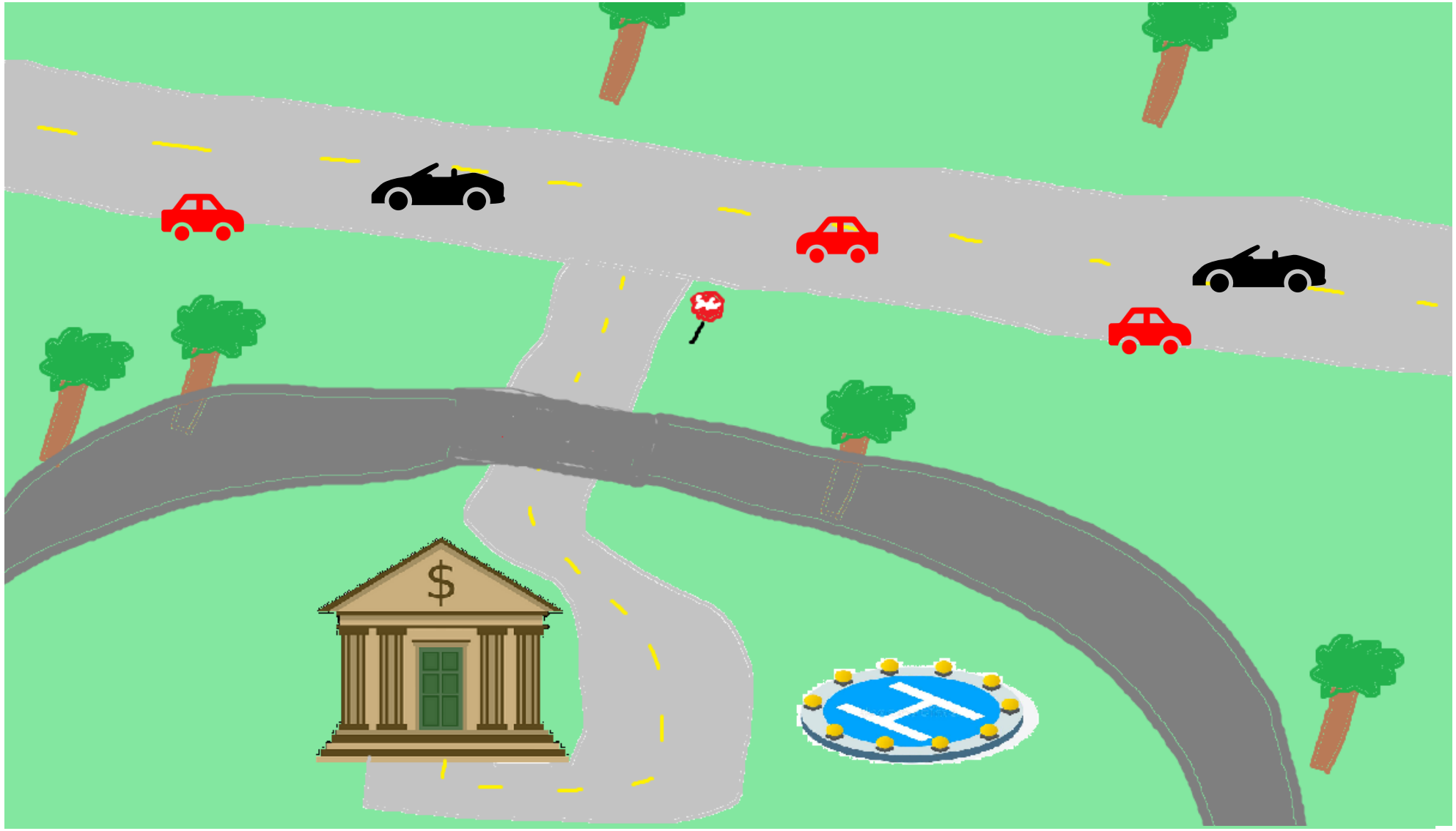
How do we know they are who they say they are?

Who can we trust?

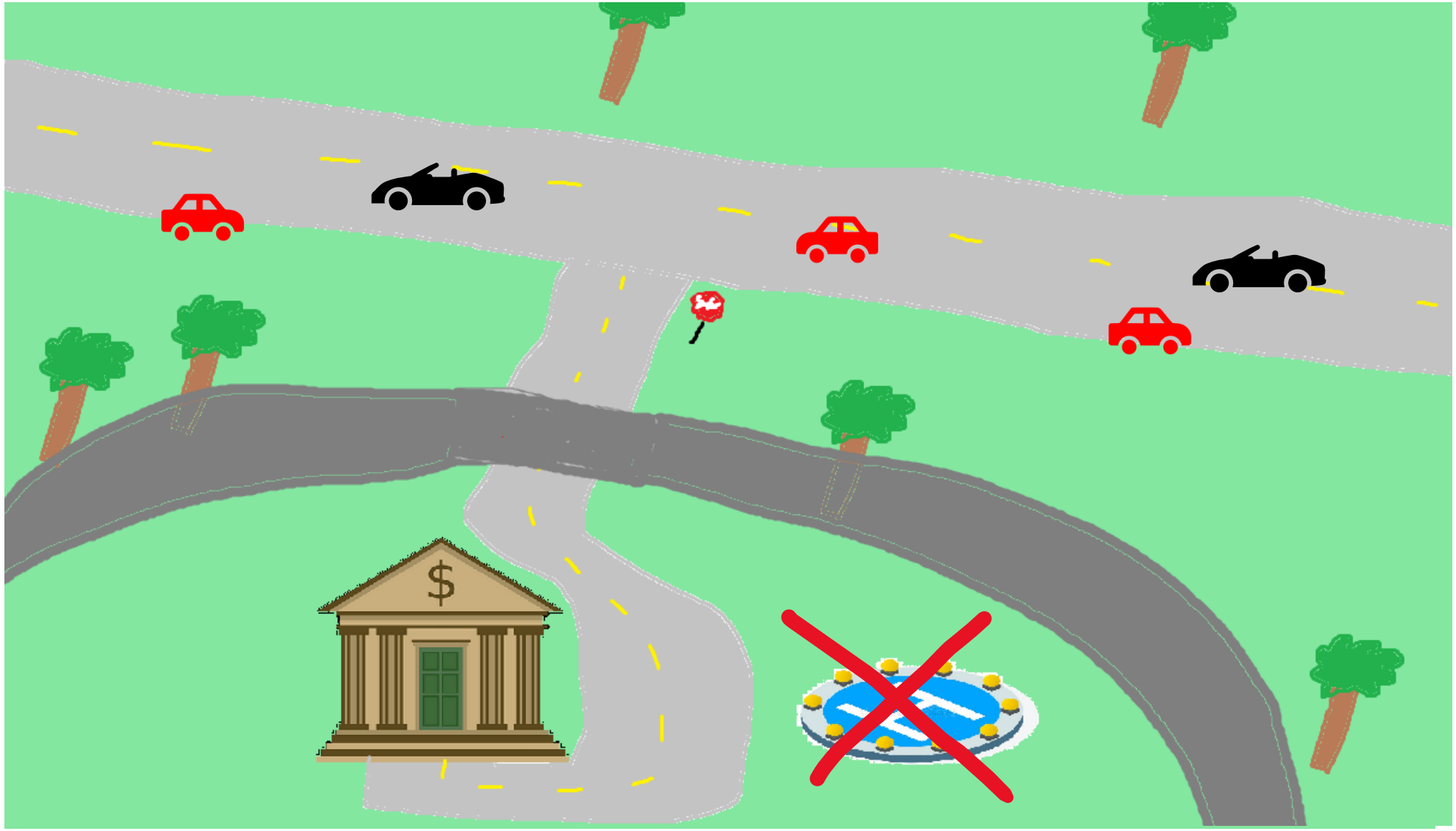




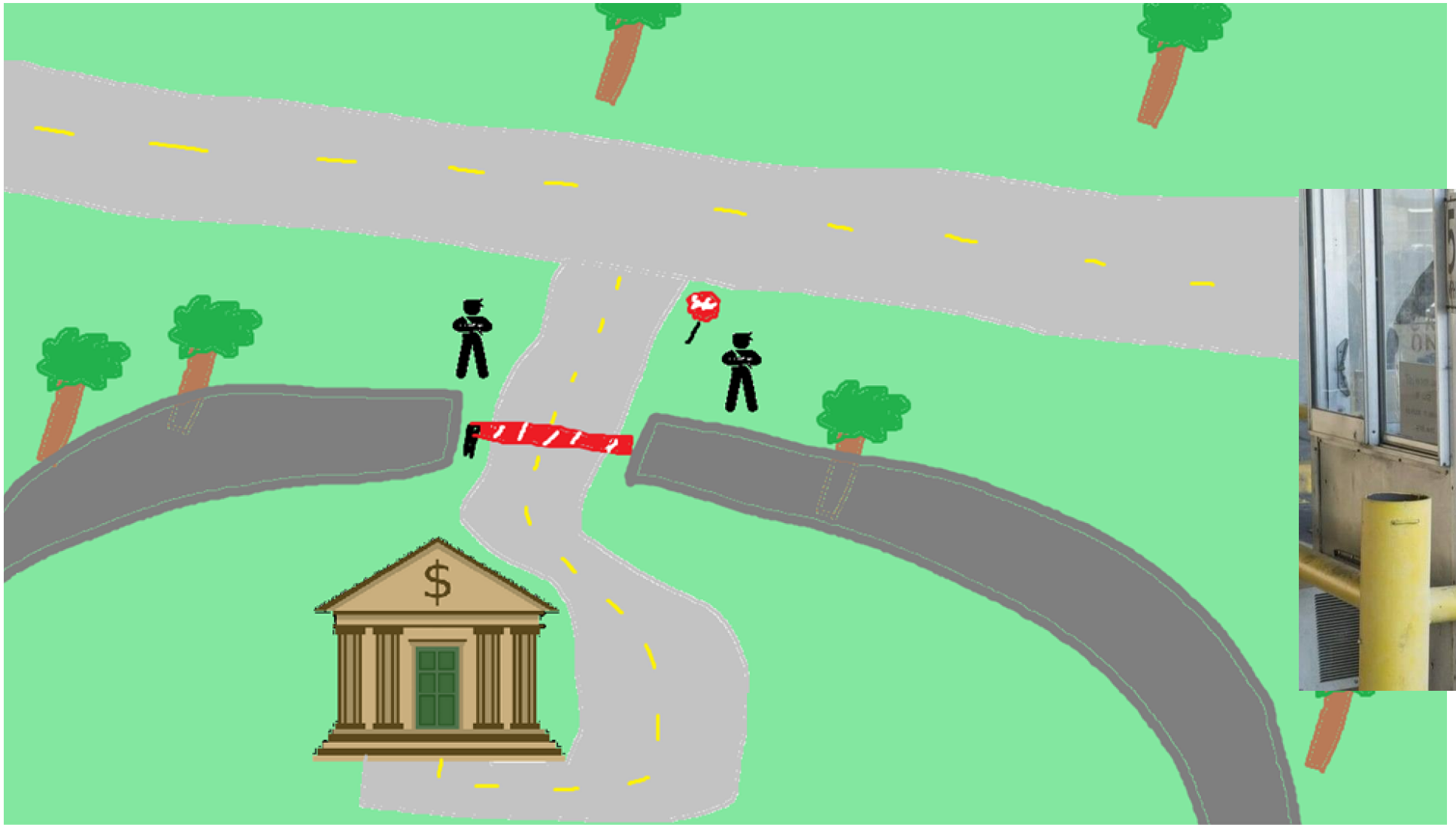
We could pretend to be someone else, steal someone else's ID, or maybe ever hack the scanner itself!



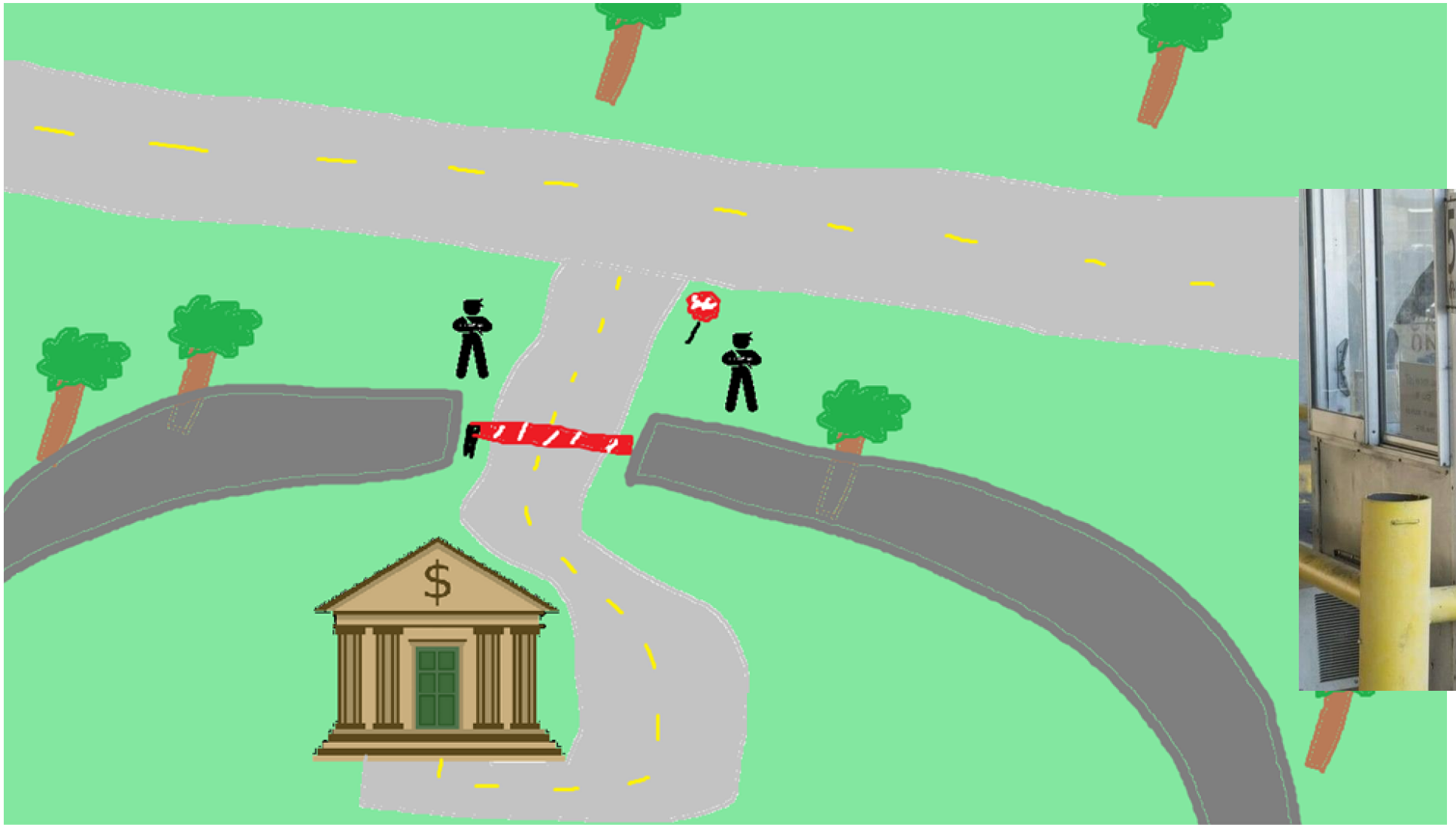
Security needs to be **accessible** and **useable**



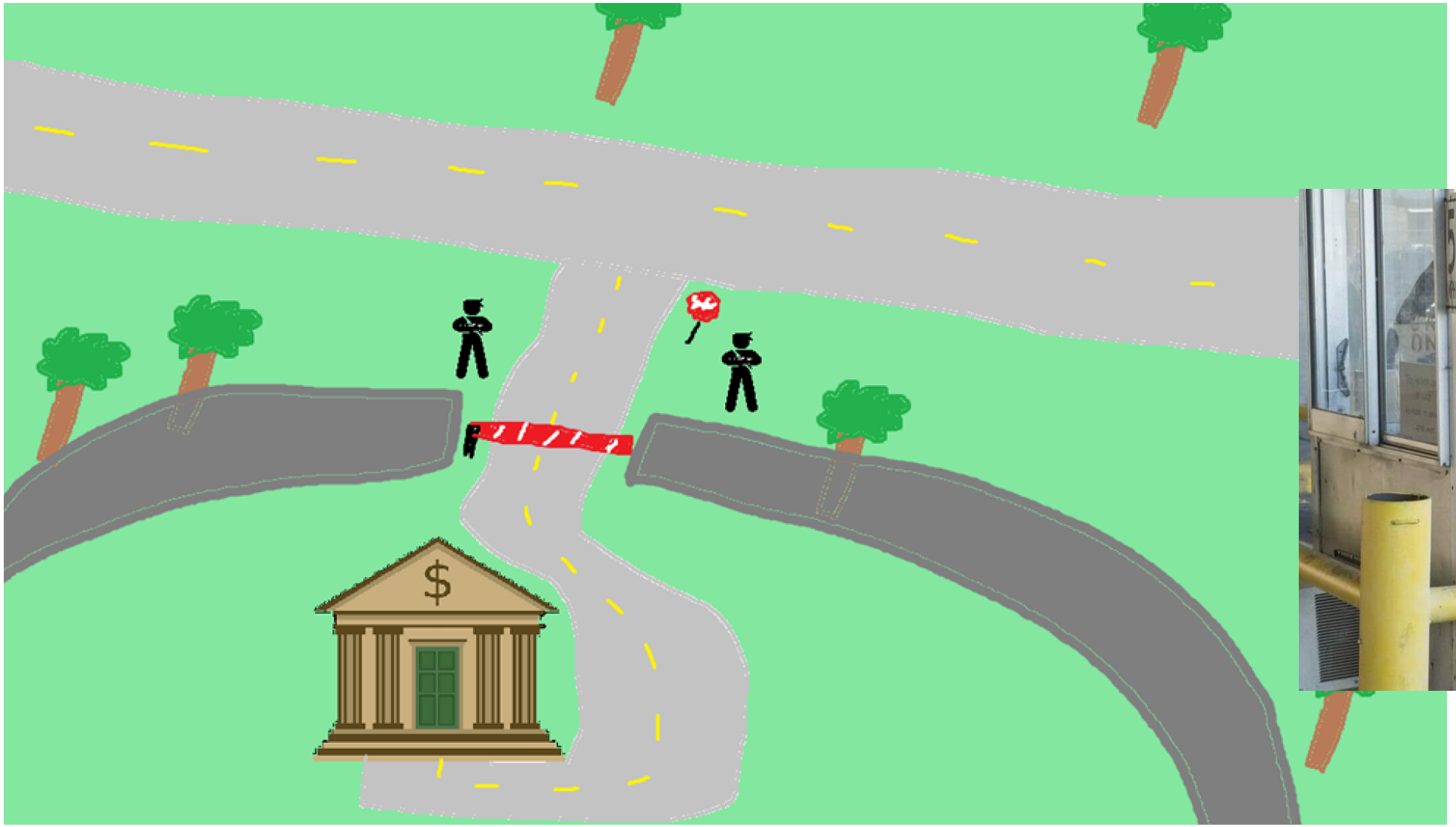
Let’s add some humans to our design!



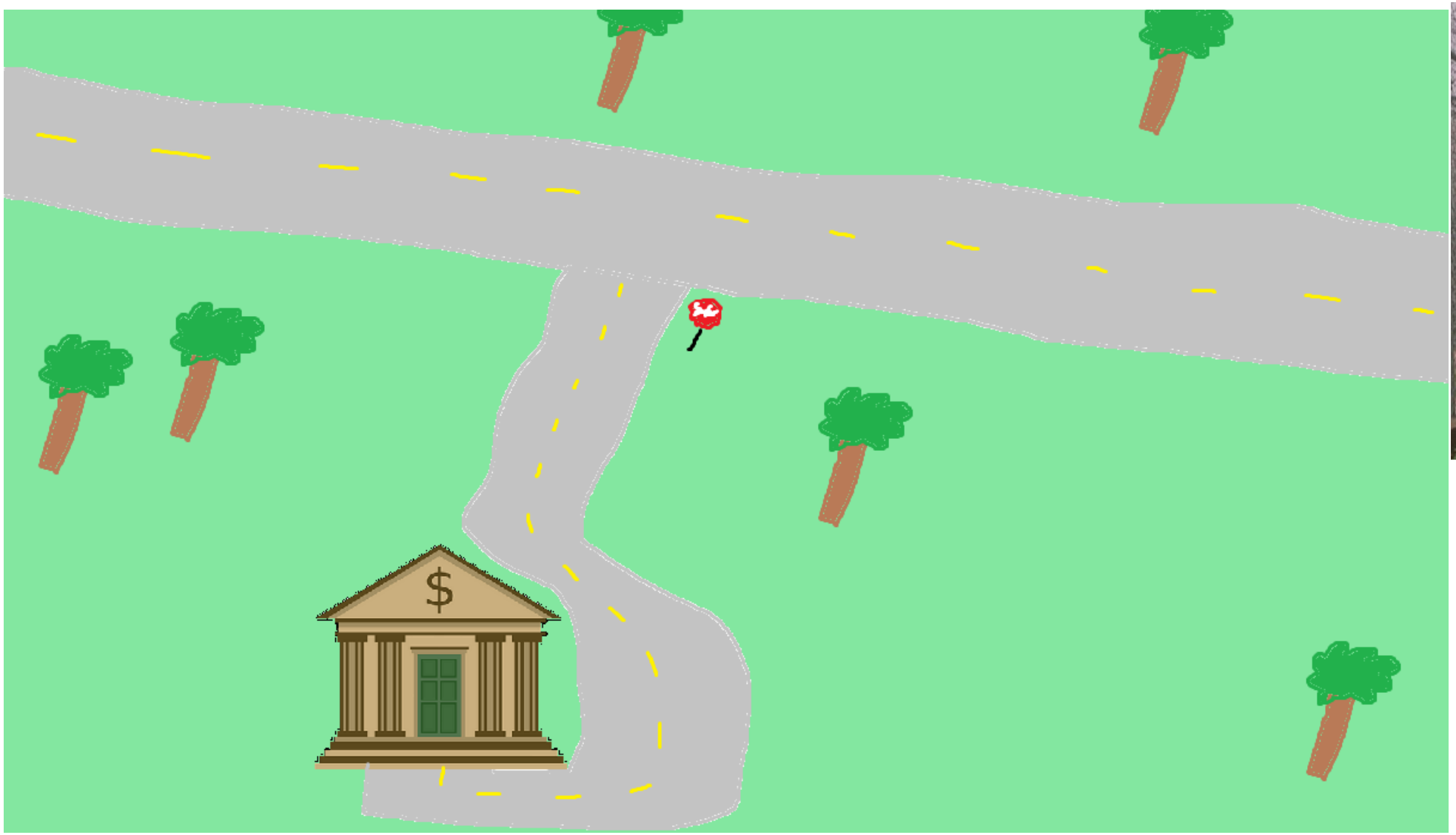
Consequences of adding humans into our design?

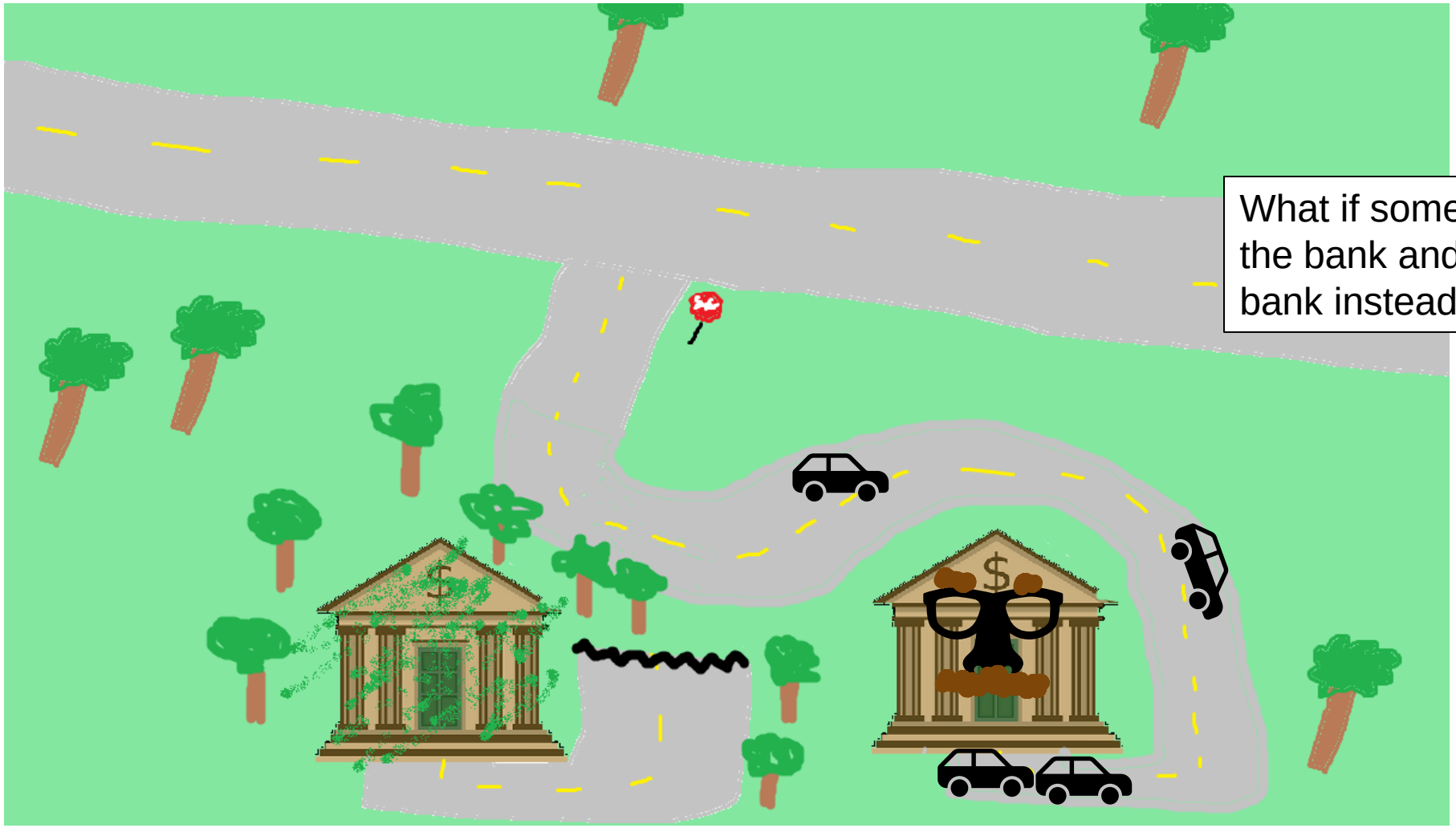


Humans can be manipulated



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





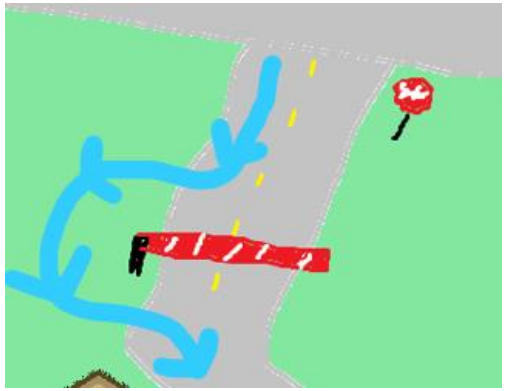
What if someone build an exact replica of the bank and tricks people to go to fake bank instead?

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

CSCI 476 Common Themes

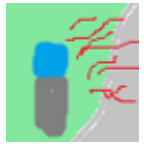
Intended Design of Software

Unpredictability of Humans



Countermeasures

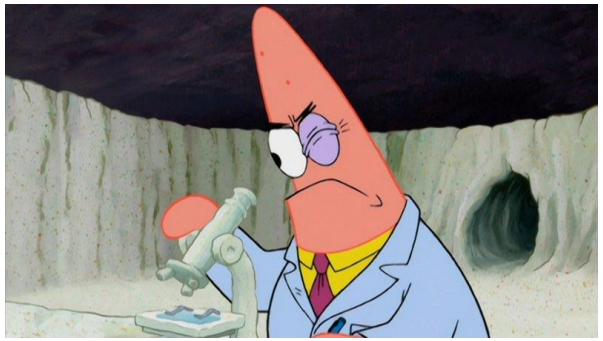
Authorization and **Trust**



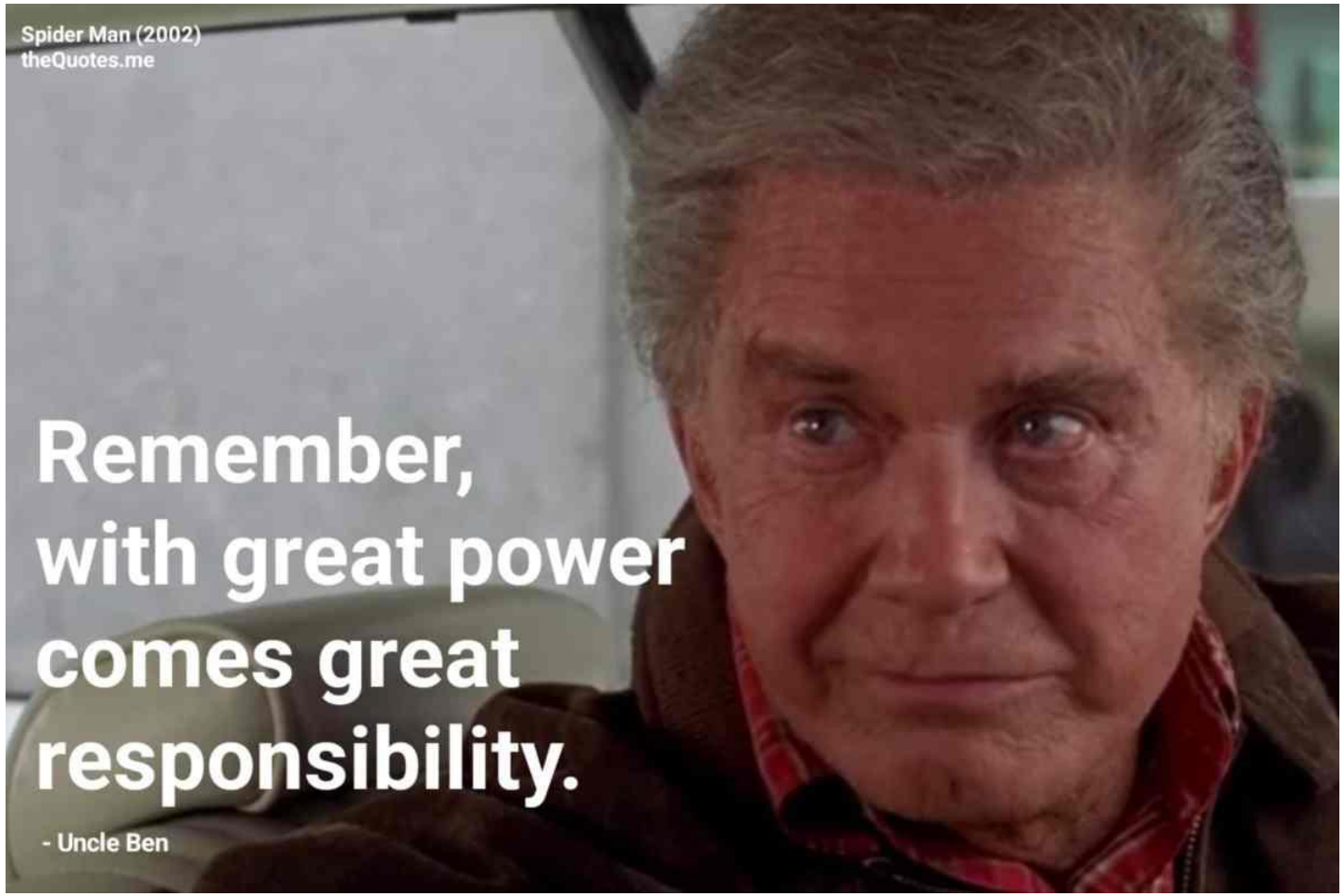
Exploitation of powerful tools and programs

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



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)

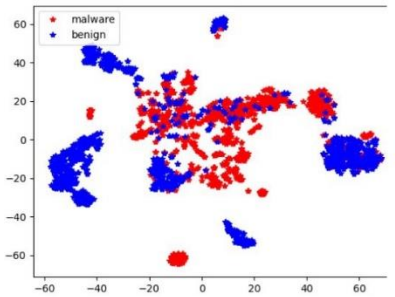
Third year Instructor @MSU
B.S & M.S @ MSU

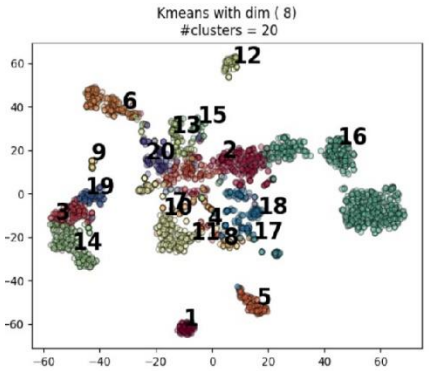
Interests
- Cybersecurity
- Malware analysis and detection
- Cybercrime
- Computer Science Education

Hometown
- Billings, MT

Teaching
- CSCI 132
- CSCI 466
- CSCI 476

Candy of choice
- Sweet tart ropes





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

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

Contact

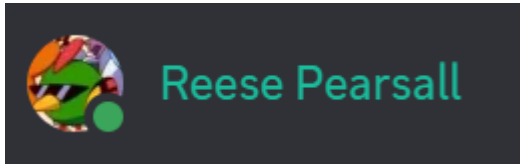
Email: reese.pearsall@montana.edu (I will respond as soon as I can)

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

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)

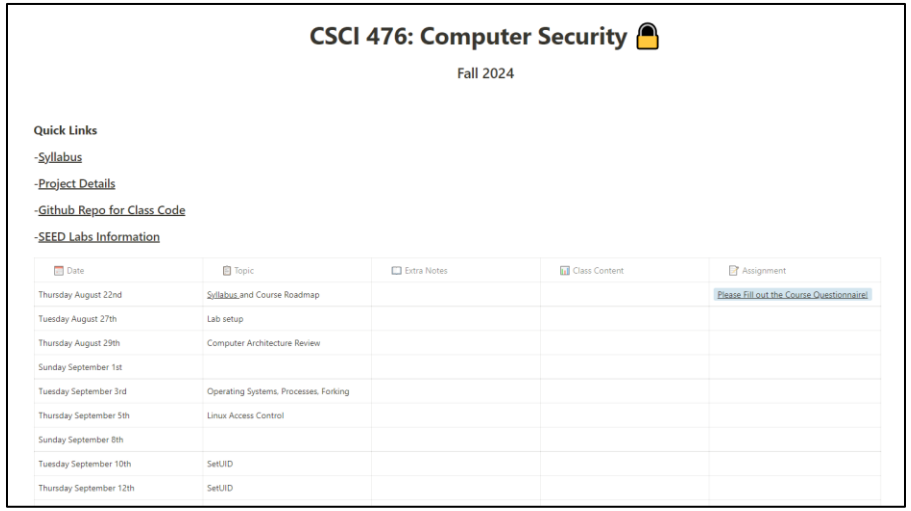


Logistics

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 2024

Quick Links

-Syllabus
-Project Details
-Github Repo for Class Code
-SEED Labs Information

Date	Topic	Extra Notes	Class Content	Assignment
Thursday August 22nd	Syllabus and Course Roadmap			Please Fill out the Course Questionnaire!
Tuesday August 27th	Lab setup			
Thursday August 29th	Computer Architecture Review			
Sunday September 1st				
Tuesday September 3rd	Operating Systems, Processes, Forking			
Thursday September 5th	Linux Access Control			
Sunday September 8th				
Tuesday September 10th	SetUID			
Thursday September 12th	SetUID			

Course Website: https://www.cs.montana.edu/pearsall/classes/fall2024/476/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

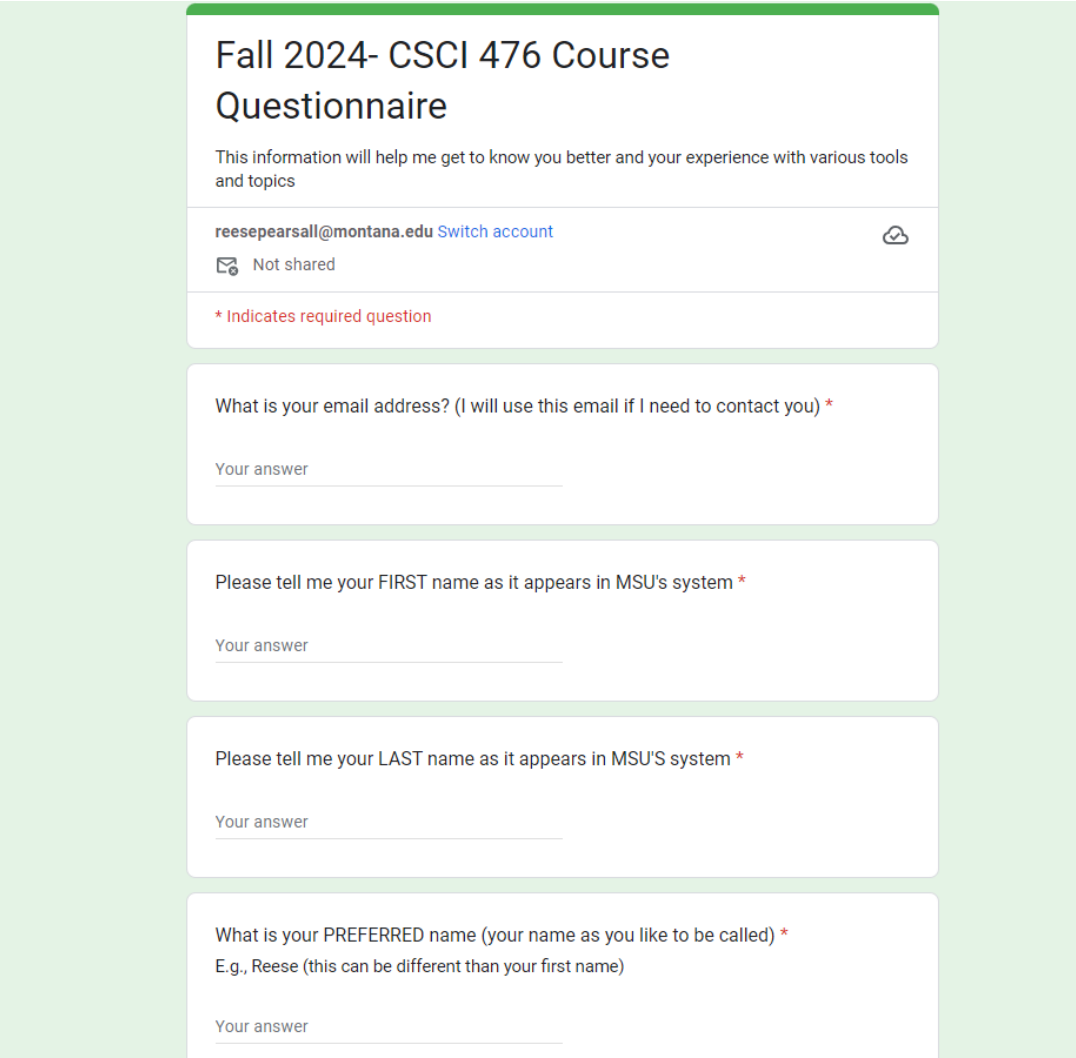
- CSCI 232- Data Structures and Algorithms
- CSCI 366- Computer Systems (recommended)
- CSCI 112- Programming in C (HIGHLY HIGHLY HIGHLY recommended)

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 2024- 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

What is your PREFERRED name (your name as you like to be called) *

E.g., Reese (this can be different than your first name)

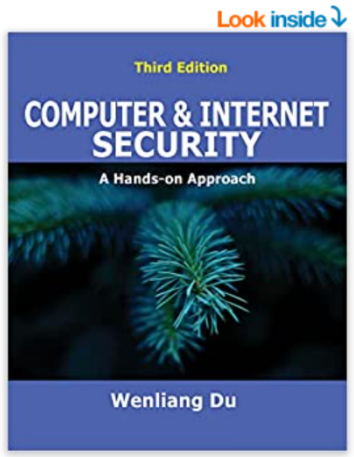
Your answer

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



See this image

Follow the Author

Wenliang Du Follow

Computer & Internet Security: A Hands-on Approach 3rd ed. Edition

by Wenliang Du (Author)

6 ratings

Part of: Computer & Internet Security (3 books)

See all formats and editions

Paperback
$62.99

4 Used from $89.03
10 New from $62.99

Teaching computer and network security principles via hands-on activities

Unique among computer security texts, this book, in its third edition, builds on the author's long tradition of teaching complex subjects through a hands-on approach. For each security principle, the book uses a series of hands-on activities to help explain the principle. Readers can touch, play with, and experiment with the principle, instead of just reading about it. The hands-on activities are based on the author's widely adopted SEED Labs, which have been used by over 1000 institutes worldwide. The author has also published online courses on Udemy based on this book.

Read more

ISBN-10	ISBN-13	Edition	Publication date	Language	Dimensions
1733003940	978-1733003940	3rd ed.	May 1, 2022	English	7.5 x 1.64 x 9.25 inches

Buy new: $62.99

FREE Returns

FREE delivery **Wednesday, January 25**

Or fastest delivery **Sunday, January 22**

Select delivery location

In Stock.

Qty: 1

Add to Cart

Buy Now

Secure transaction

Ships from Amazon.com
Sold by Amazon.com

Return policy: Eligible for Return, Refund or Replacement within 30 days of receipt

Support: Free Amazon product support included

prime Enjoy fast, FREE delivery, exclusive deals and award-winning

- 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

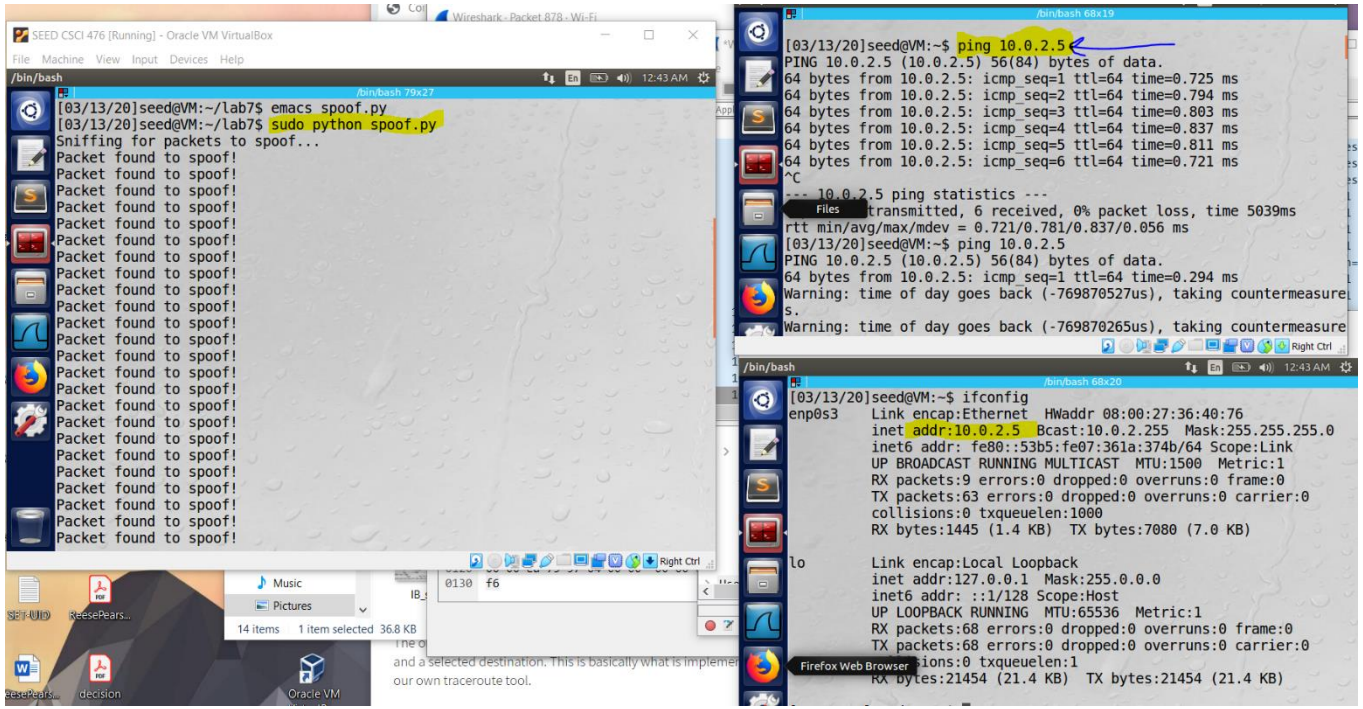
If you prefer to create a SEED VM on your local computers, there are two ways to do that: (1) use a pre-built SEED VM; (2) create a SEED VM from scratch.

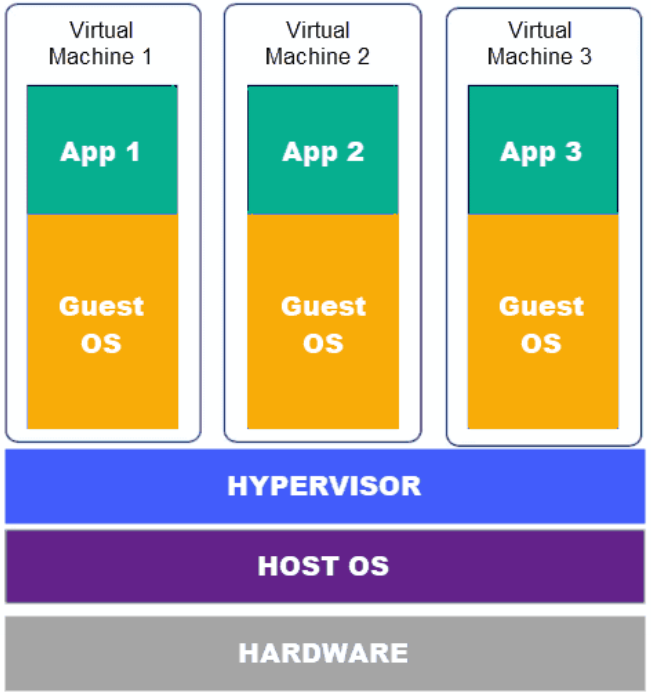
Approach 1: Use a pre-built SEED VM. We provide a pre-built SEED Ubuntu 20.04 VirtualBox image (`SEED-Ubuntu20.04.zip`, size: 4.0 GB), which can be downloaded from the following links.

- 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 (10)
- 15% Research Project
- 15% Final Exam

Grading

- **70% Labs** (10)

➢ 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 Brightspace 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 November 21st

➢ 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)

➢ You get to use a note sheet

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, Academic Misconduct, Generative AI tools

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 another person and modify it

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

Do not use any tools or AI that will write code or solutions for you

Using small snippets of code from the internet is acceptable *(but should not be needed).* If you do use a small snippet of code from the internet, you should leave a reference as a comment in your code

MSU Resources

https://www.cs.montana.edu/pearsall/classes/msu_resources.html

Diversity Statement

Montana State University's campuses are committed to providing an environment that emphasizes the dignity and worth of every member of its community and that is free from harassment and discrimination based upon race, color, religion, national origin, creed, service in the uniformed services (as defined in state and federal law), veteran's status, sex, age, political ideas, marital or family status, pregnancy, physical or mental disability, genetic information, gender identity, gender expression, or sexual orientation. Such an environment is necessary to a healthy learning, working, and living atmosphere because discrimination and harassment undermine human dignity and the positive connection among all people at our University. Acts of discrimination, harassment, sexual misconduct, dating violence, domestic violence, stalking, and retaliation will be addressed consistent with this policy.

Inclusivity Statement

I support an inclusive learning environment where diversity and individual differences are understood, respected, appreciated, and recognized as a source of strength. We expect that students, faculty, administrators and staff at MSU will respect differences and demonstrate diligence in understanding how other peoples' perspectives, behaviors, and worldviews may be different from their own.

Counseling

In addition to eating right, taking breaks when you need them, and getting enough sleep, you may benefit from talking to a professional counselor if you think stress could be impacting your health. Here is a blurb and some links from MSU's Counseling & Psychological Services: MSU strives to create a culture of support and recognizes that your mental health and wellness are equally as important as your physical health. We want you to know that it's OK if you experience difficulty, and there are several resources on campus to help you succeed emotionally, personally, and academically:

- Counseling & Psychological Services: montana.edu/counseling
- Health Advancement: montana.edu/oha
- Insight Program (Substance Use): montana.edu/oha/insight
- Suicide Prevention: montana.edu/suicide-prevention
- Medical Services: montana.edu/health/medical.html
- WellTrack: montana.welltrack.com/register

Civil Rights

There should be no discrimination or harassment for anyone at MSU. If you notice anything that seems to violate that principle, the Office of Institutional Equity can help. As an employee of MSU, I am a mandatory reporter, which means if I learn of any discrimination or harassment at MSU, I am obligated by my contract to report it.

Hamilton Hall, Offices 114, 116, and 118

How to do well in this class

- **Get started on labs early**
- Get help when you need it
- Come to class and office hours]
- Take care of yourself
- **Try to have fun**

Questions?