CSCI 476: Computer Security

Lecture 1: Introduction, Syllabus, and Logistics

Reese Pearsall

Fall 2022

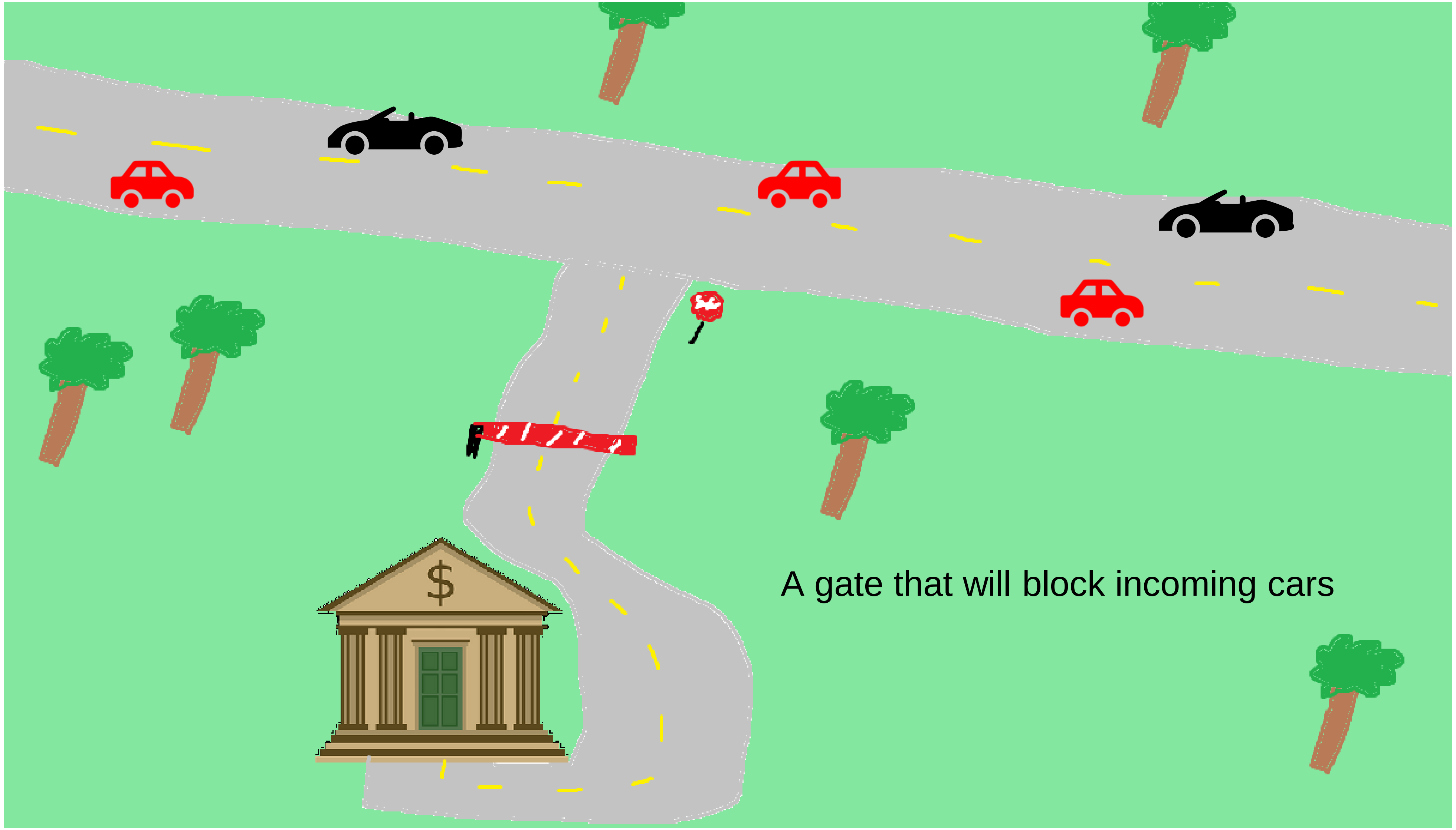
Before we jump into course rules, we will do a short exercise to get you thinking about security

Securing an asset

We need to secure the area around the bank

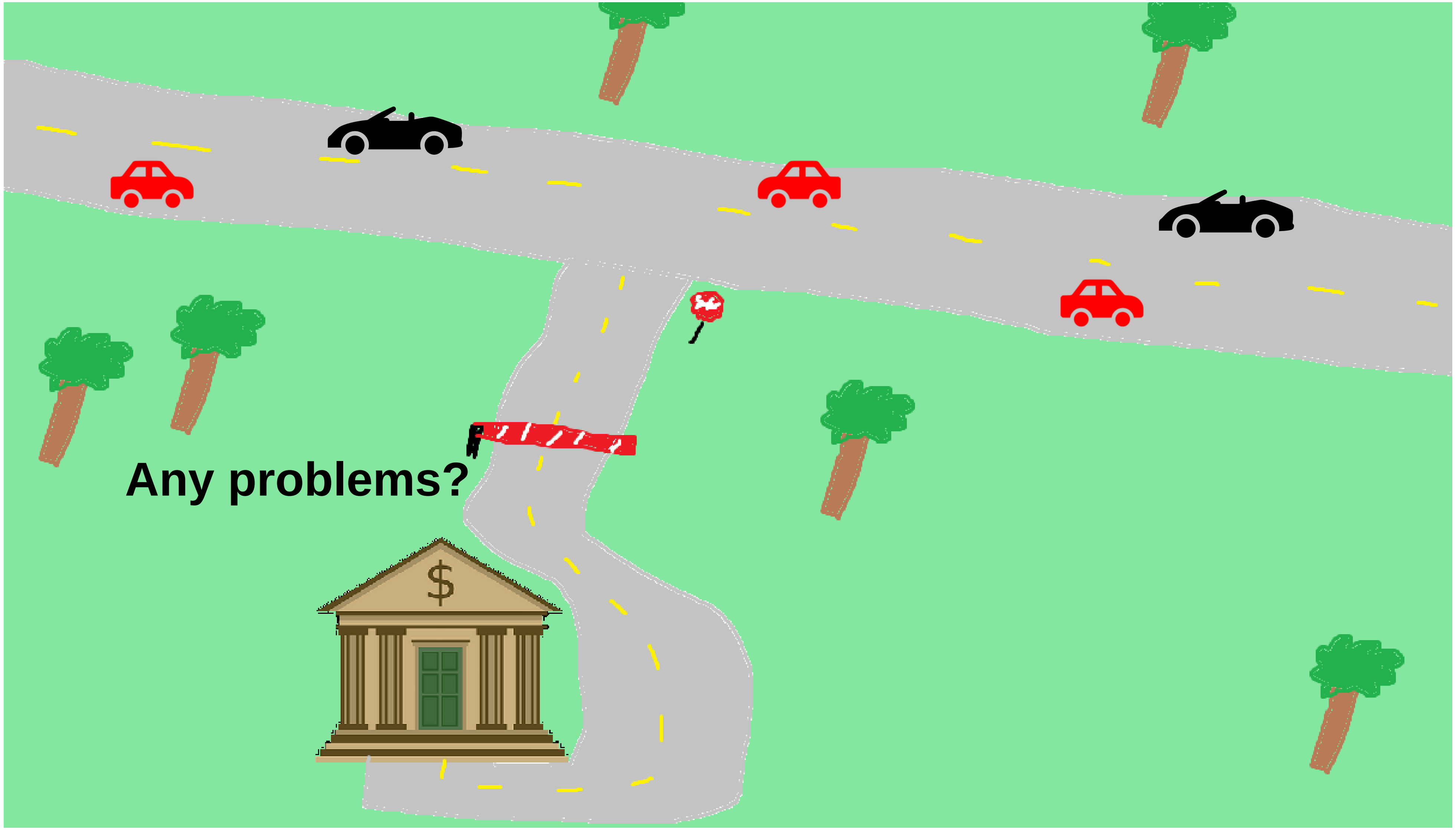
Only people that are allowed should be able to pass into the bank

Securing an asset



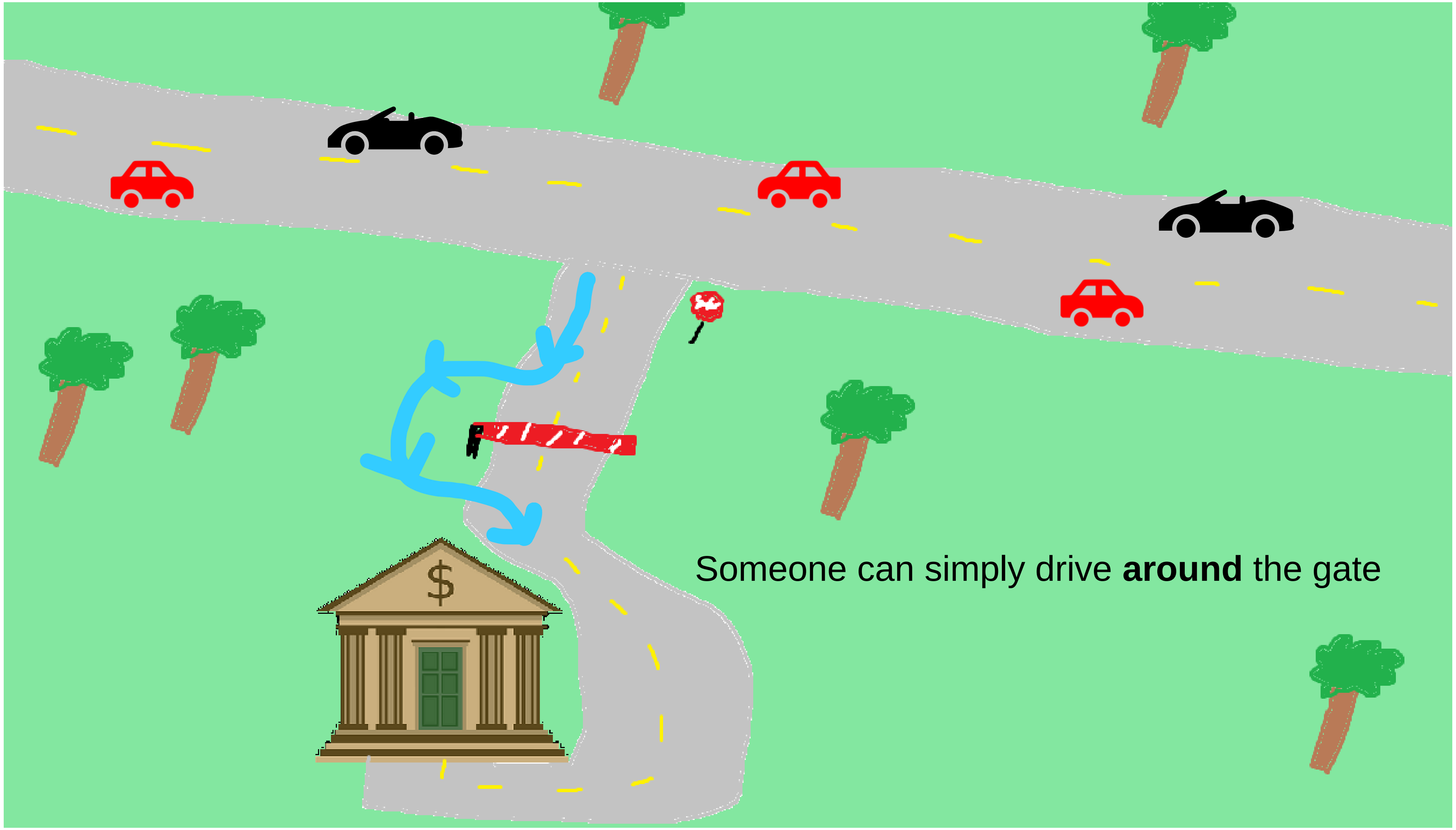
A gate that will block incoming cars

Securing an asset



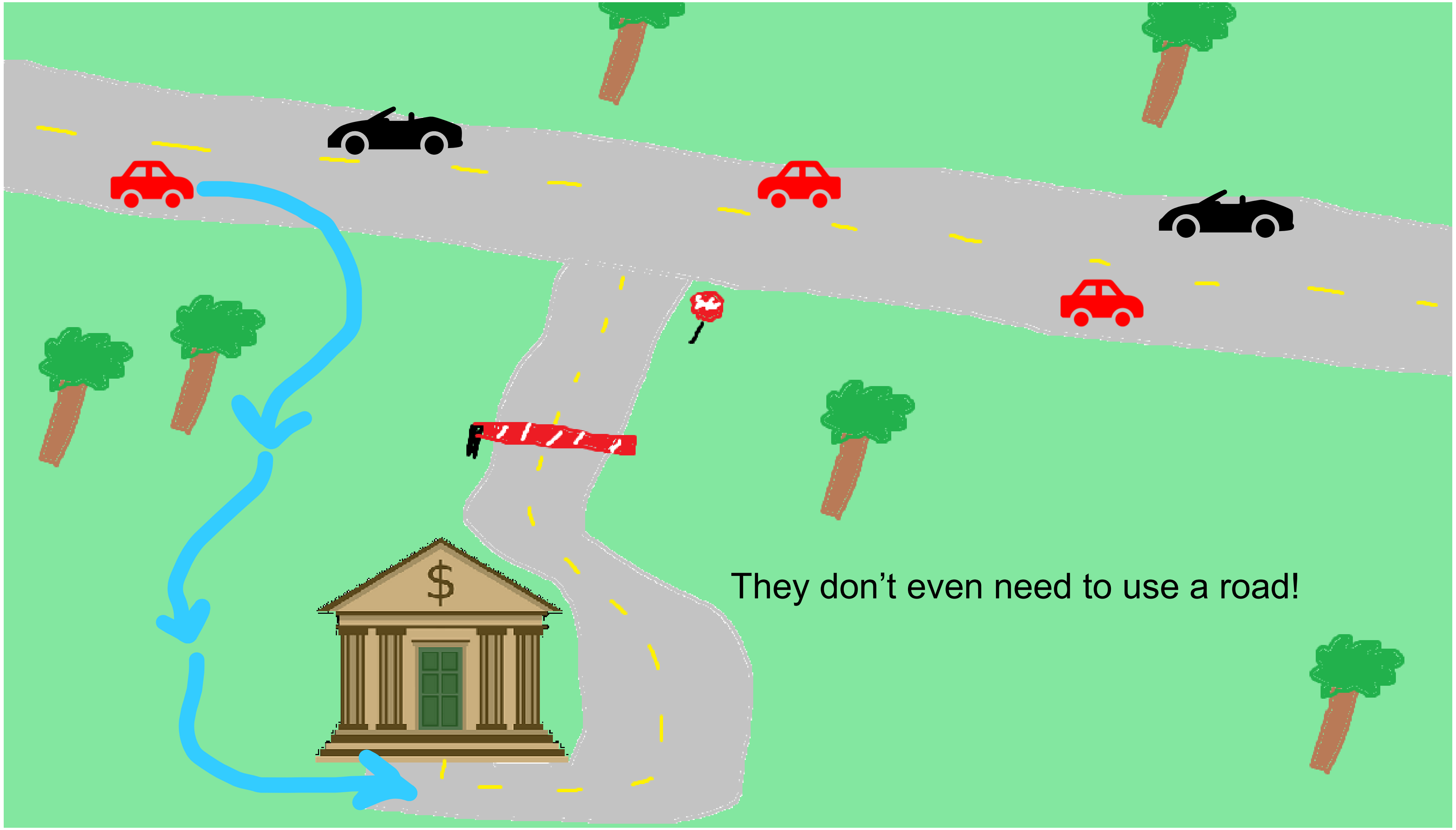
Any problems?

Securing an asset



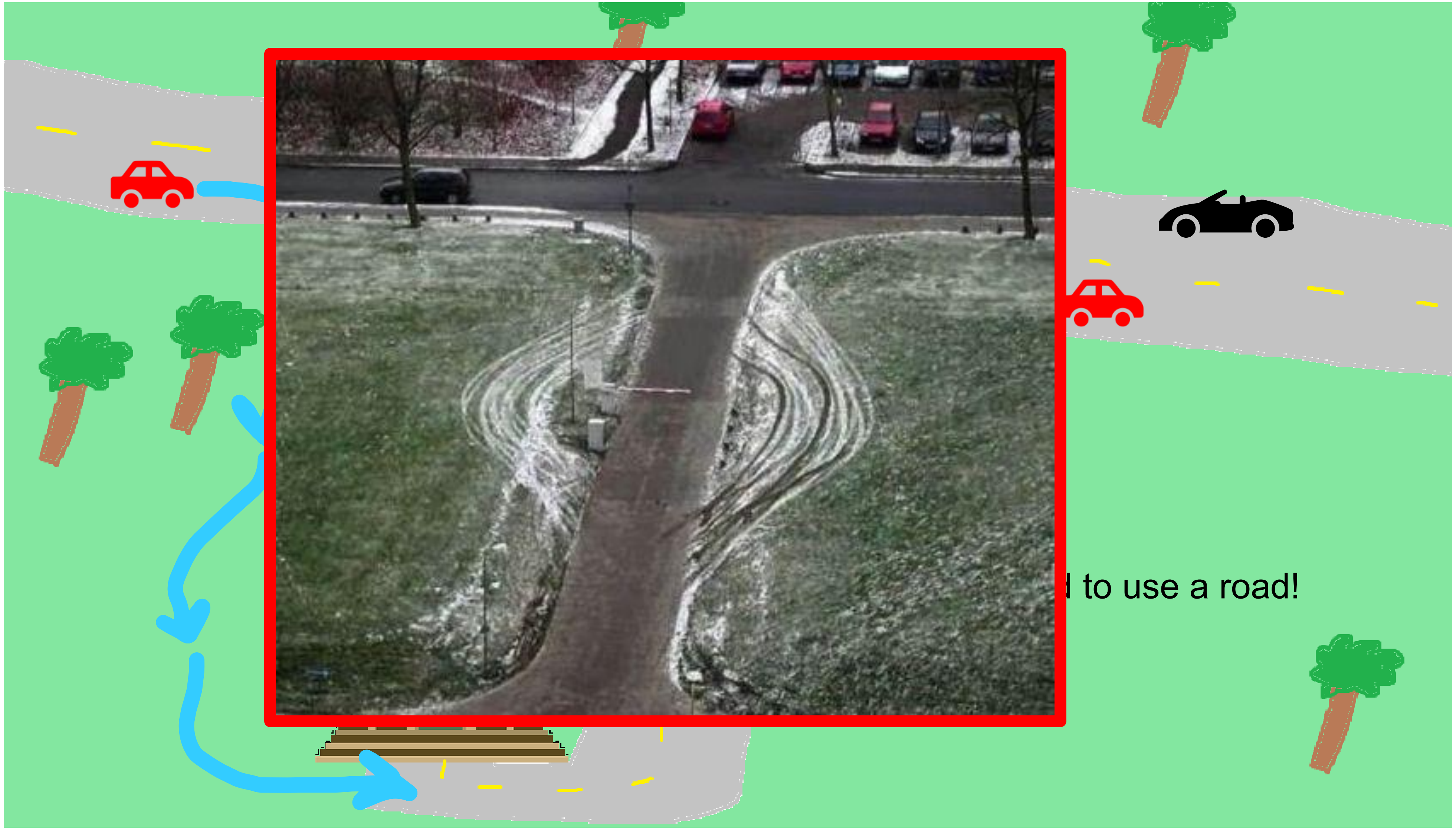
Someone can simply drive **around** the gate

Securing an asset



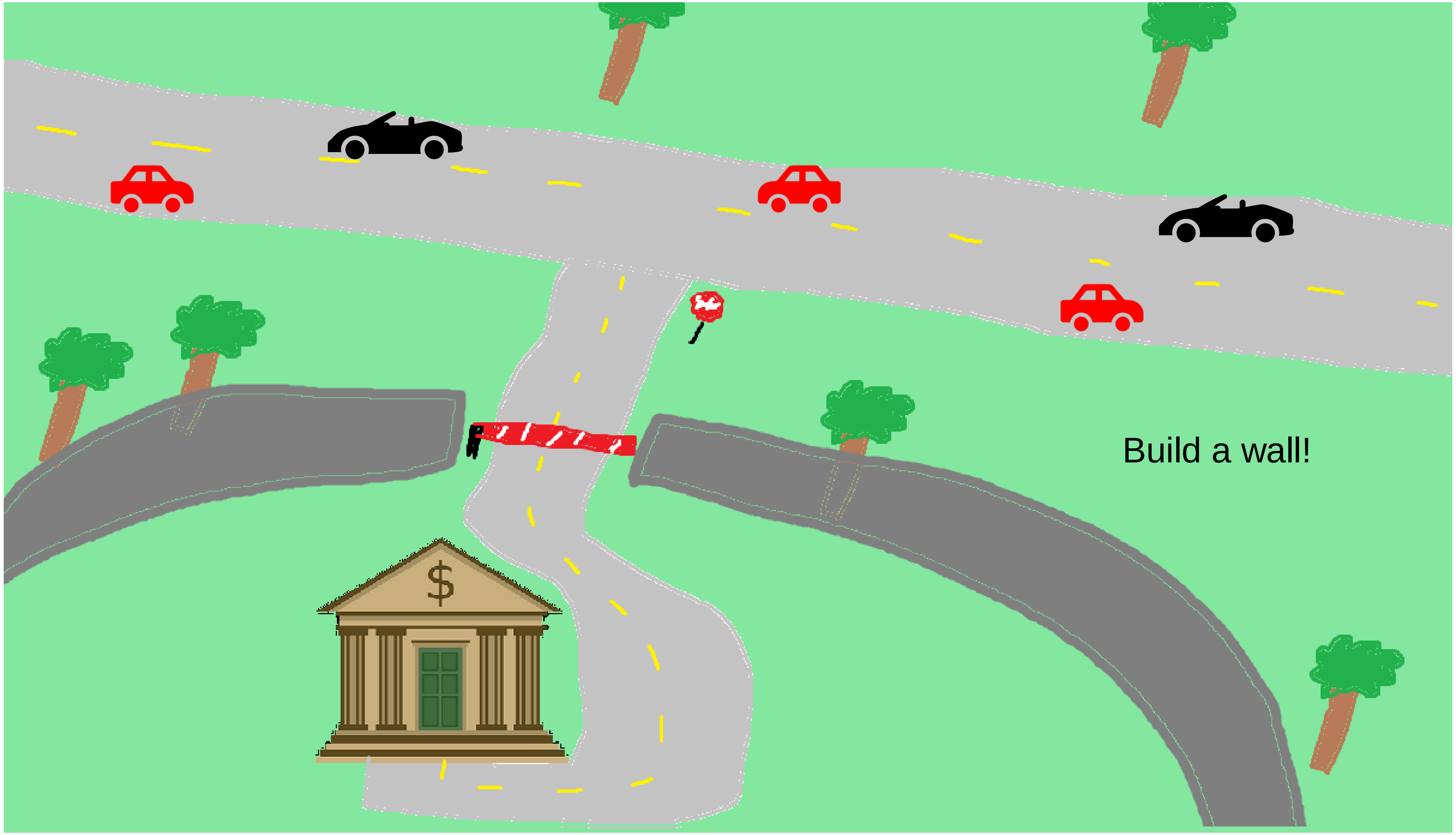
They don’t even need to use a road!

Securing an asset



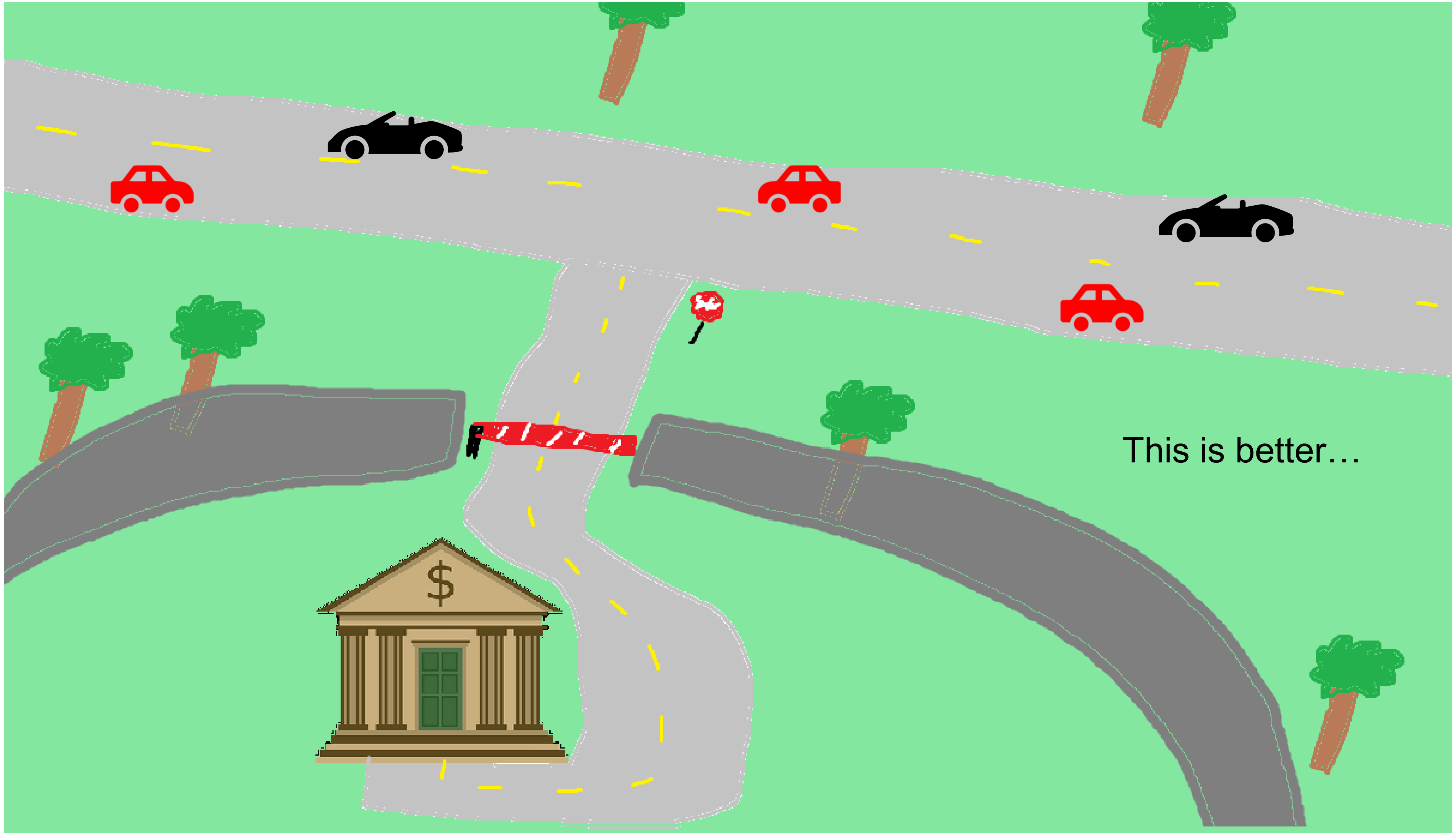
to use a road!

Securing an asset



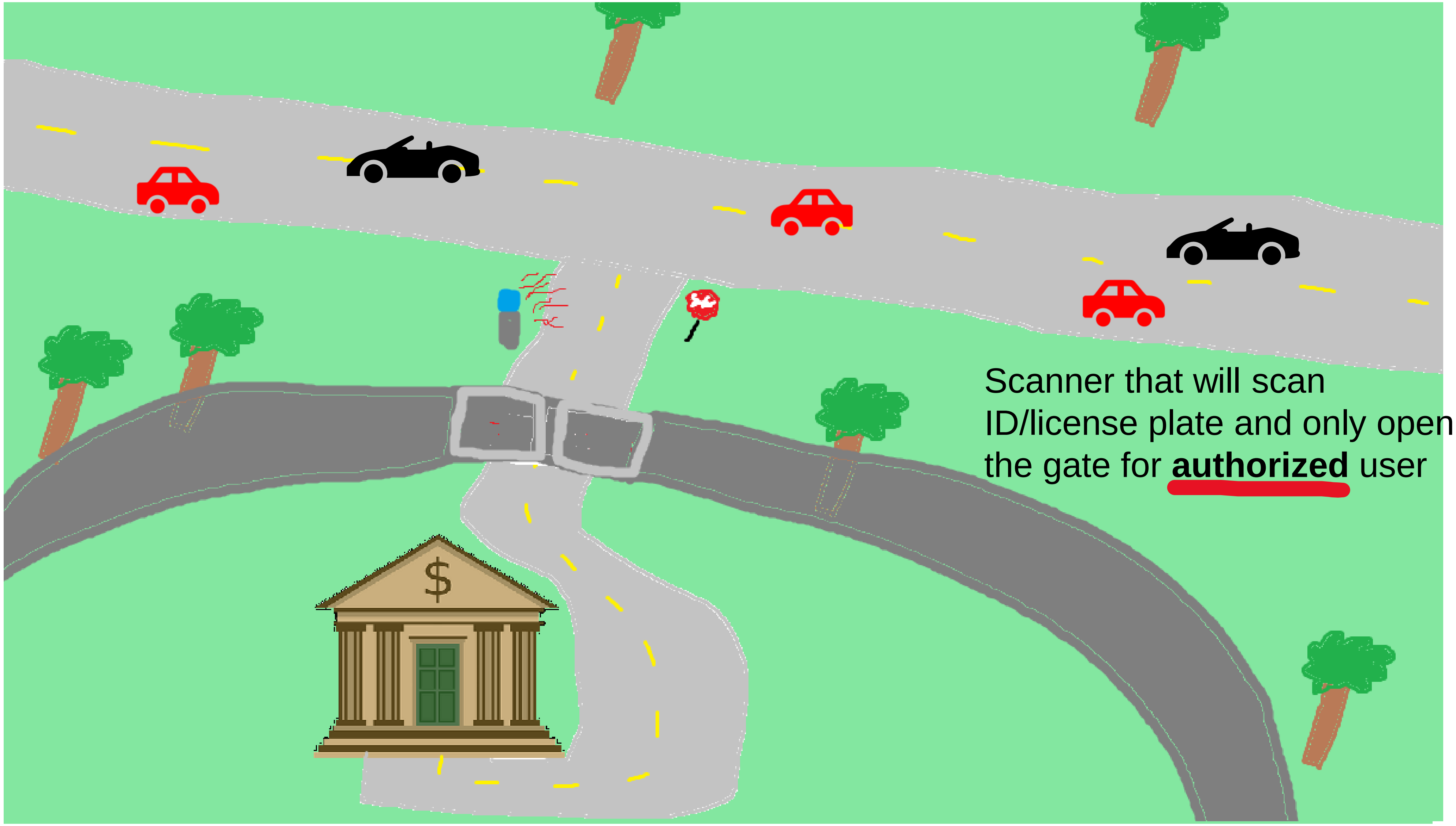
Build a wall!

Securing an asset



This is better…

Securing an asset



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

Securing an asset

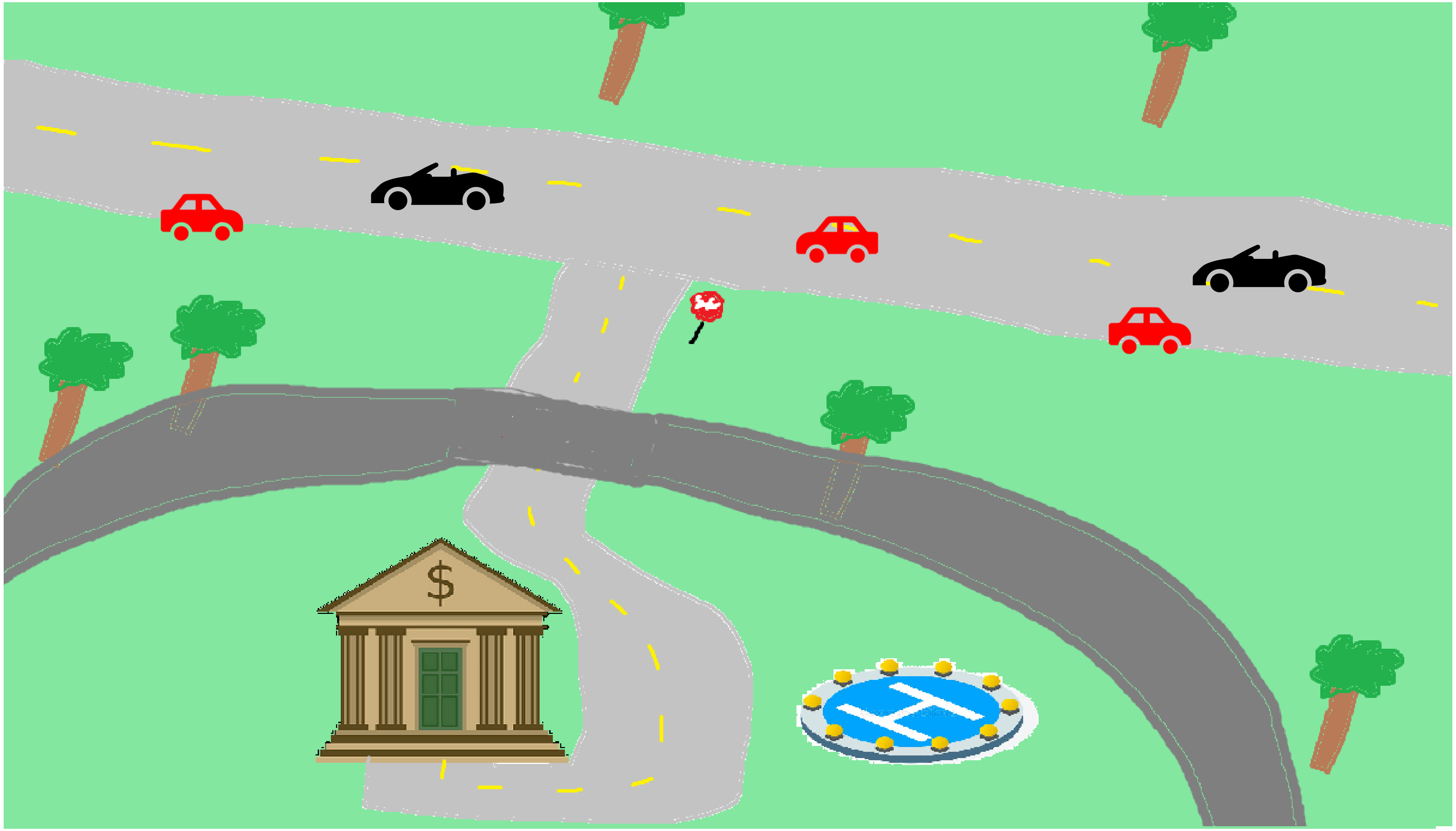
How do we know they are who they say they are?

Securing an asset

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

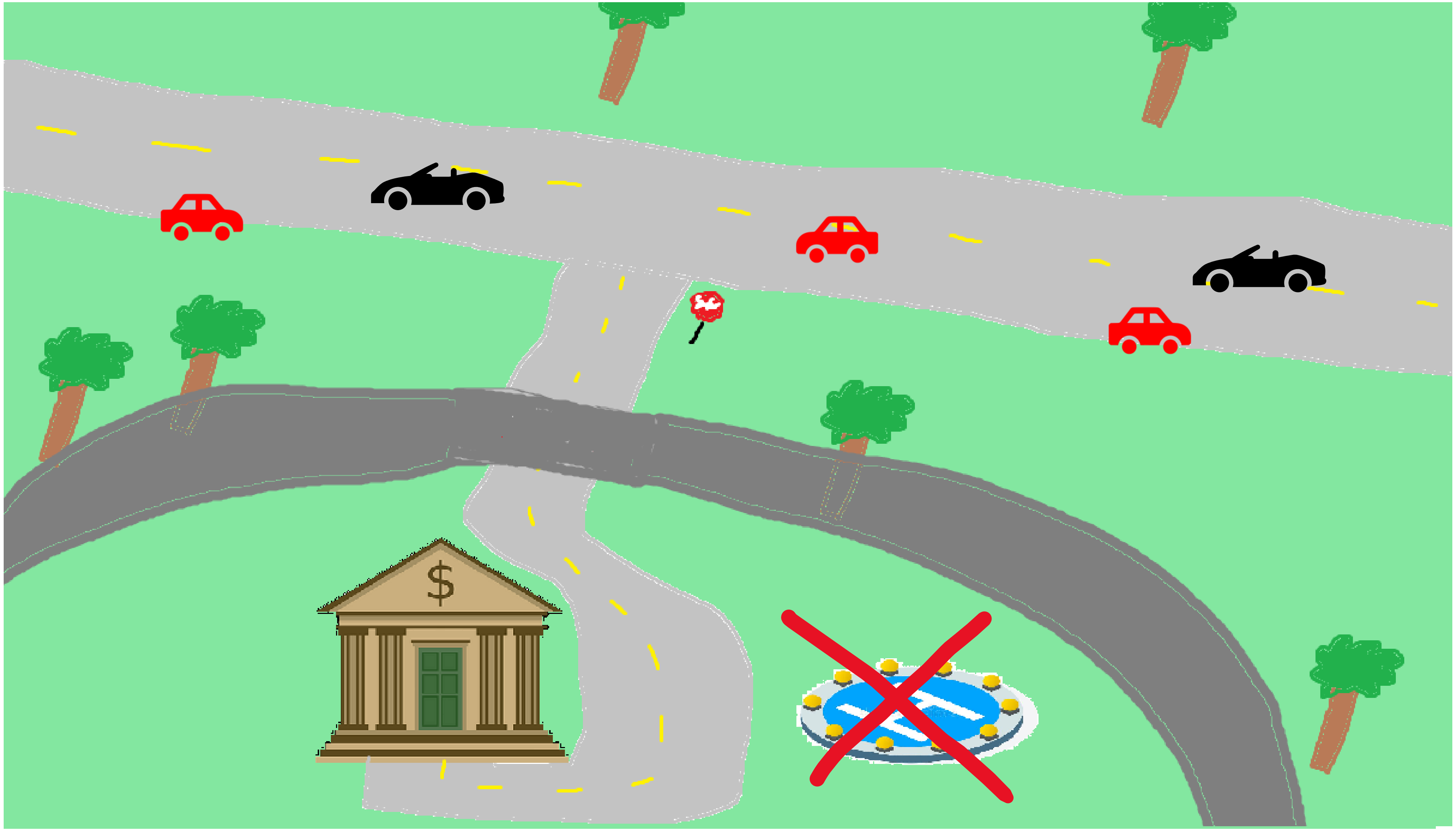
AUTHENTICATION

Securing an asset

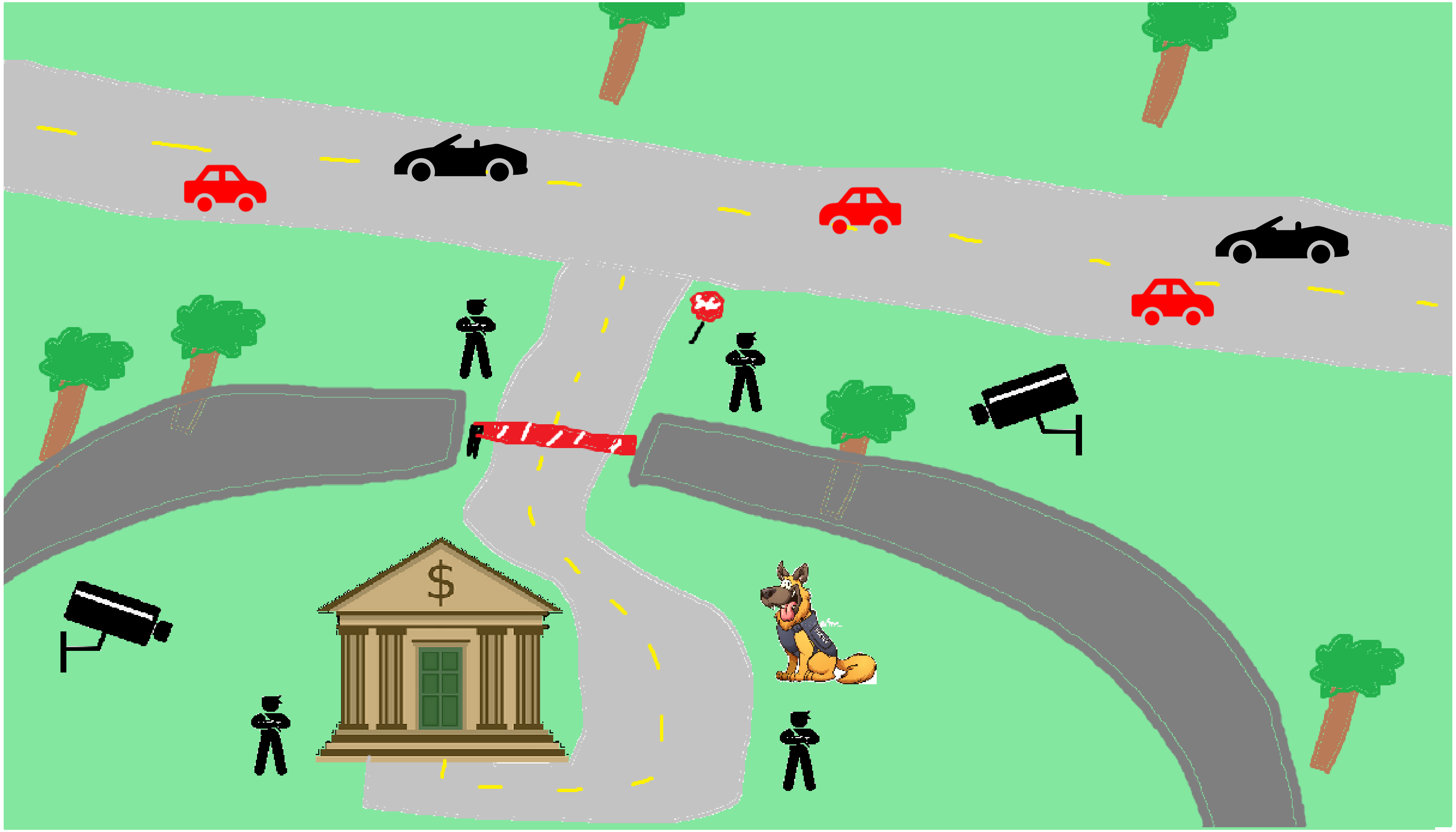


Securing an asset

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

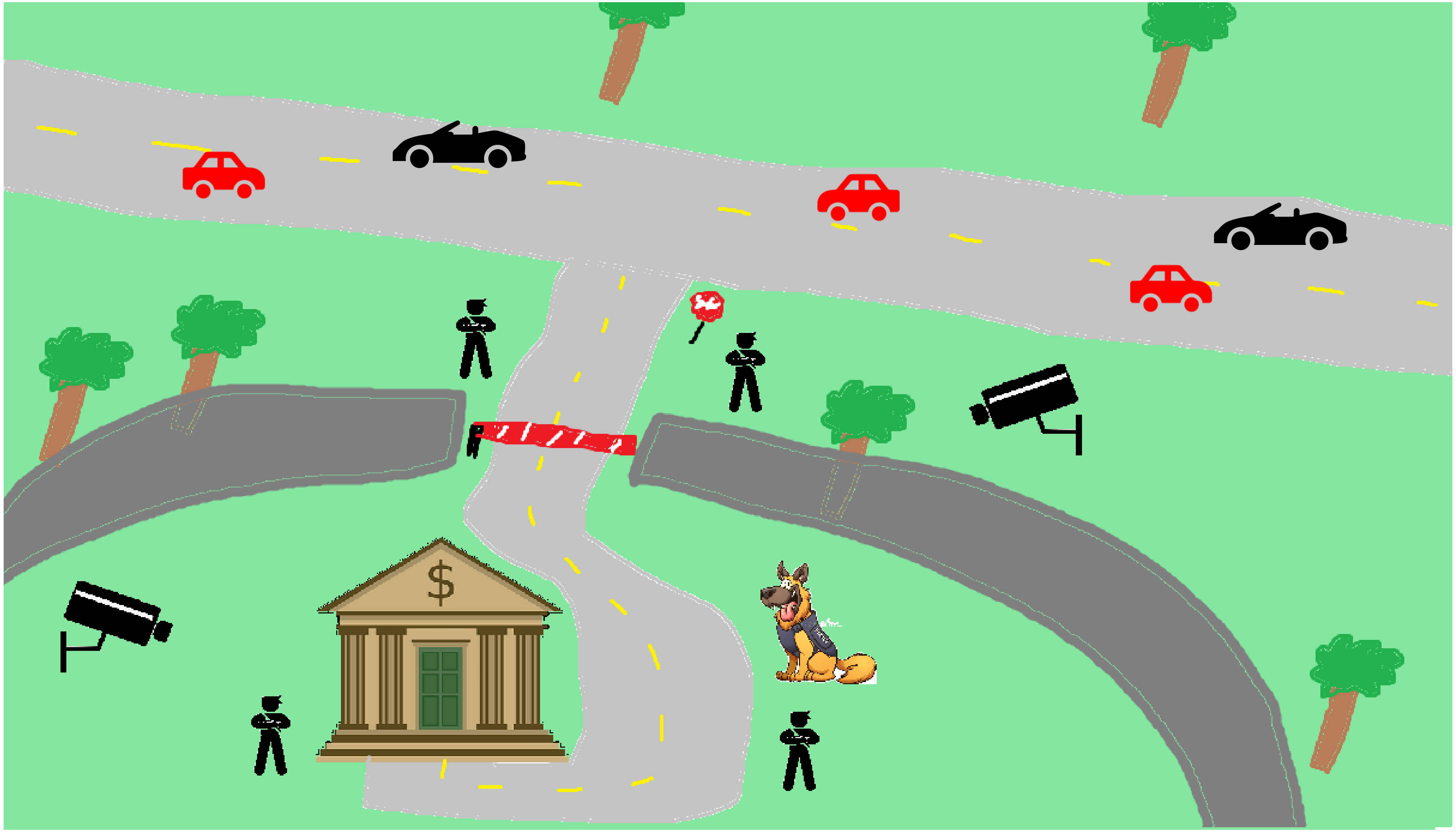


Securing an asset



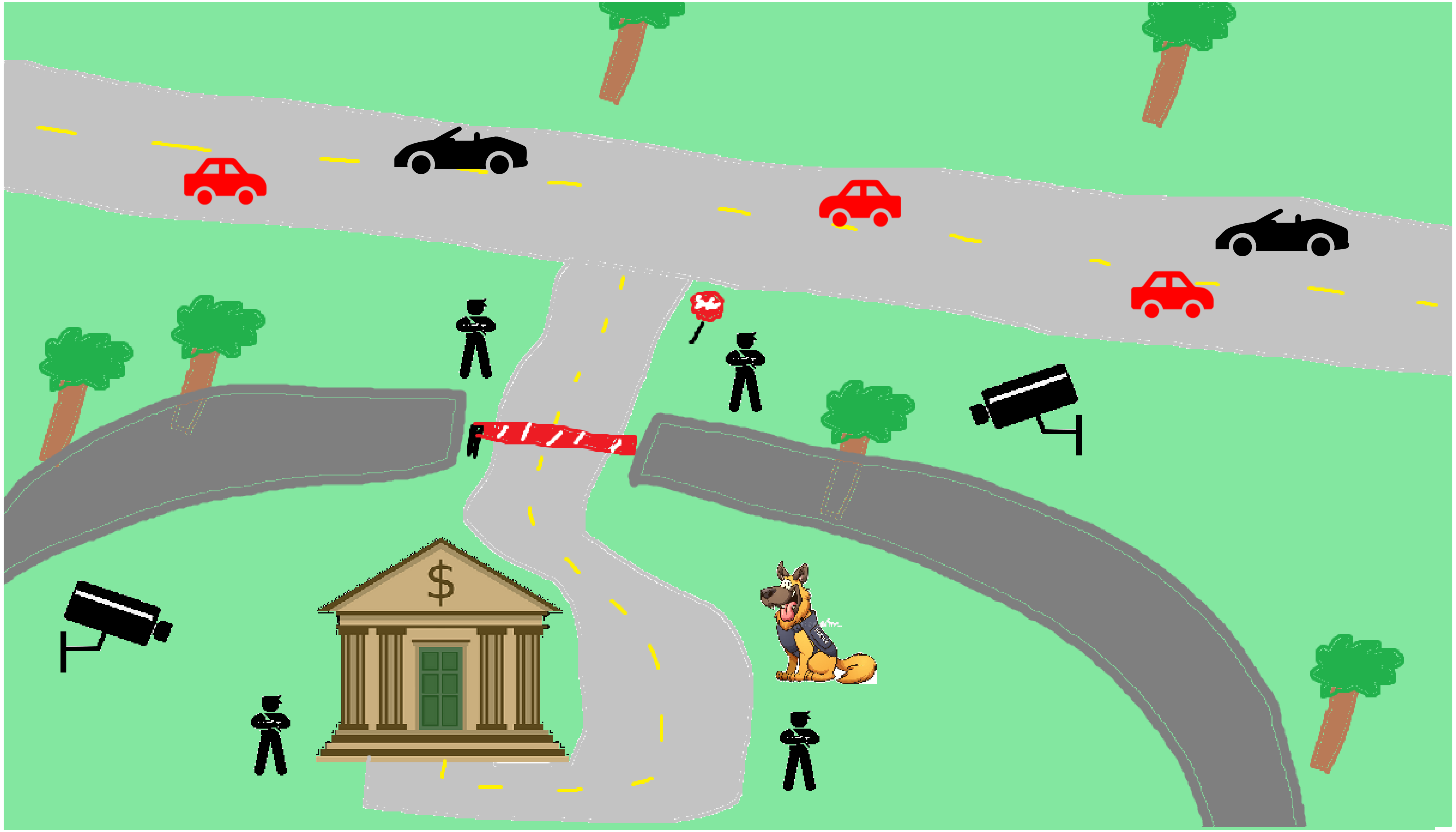
Securing an asset

Actively seeking out potential threats ✓



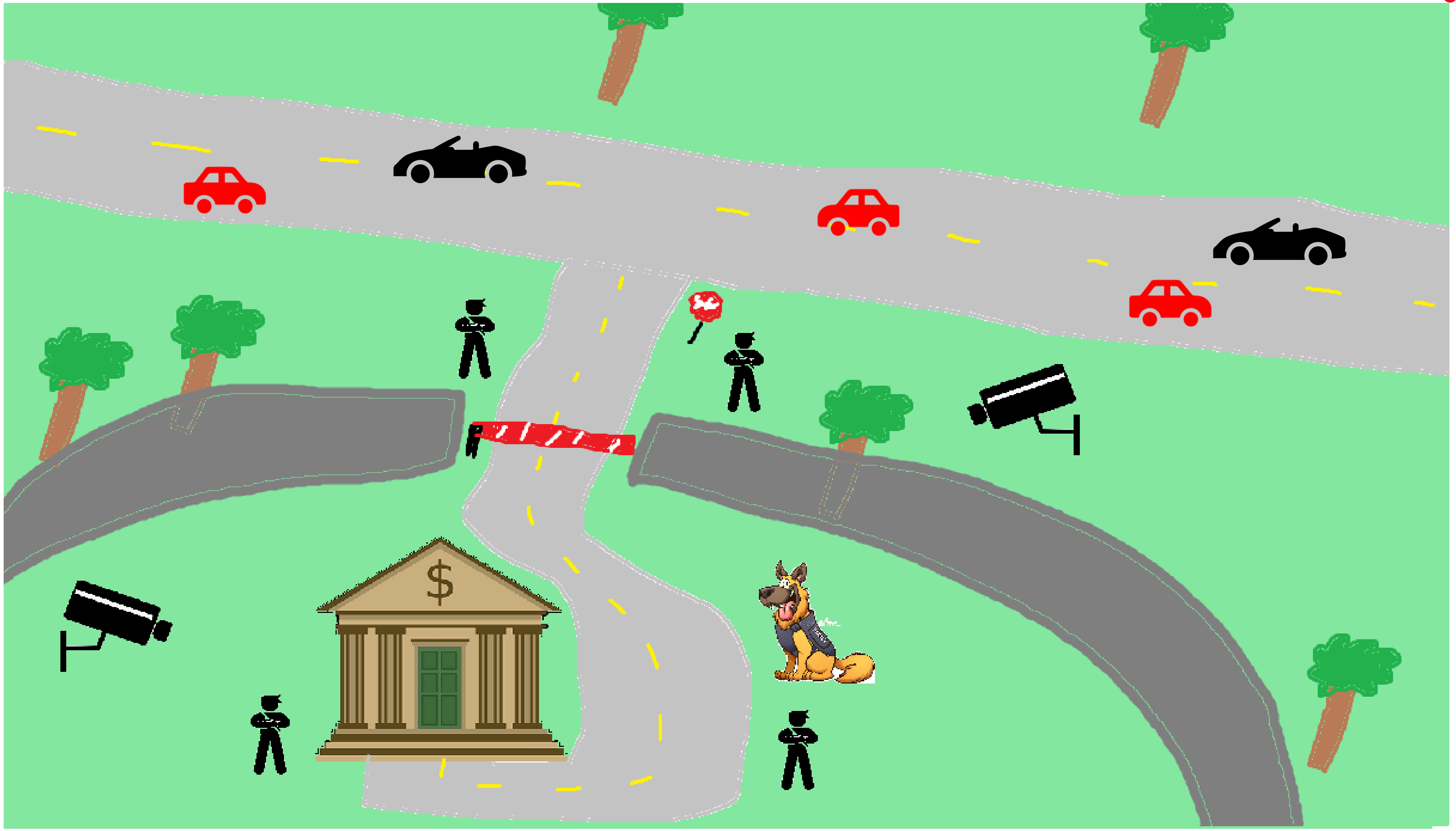
Securing an asset

Consequences of adding humans into our design?

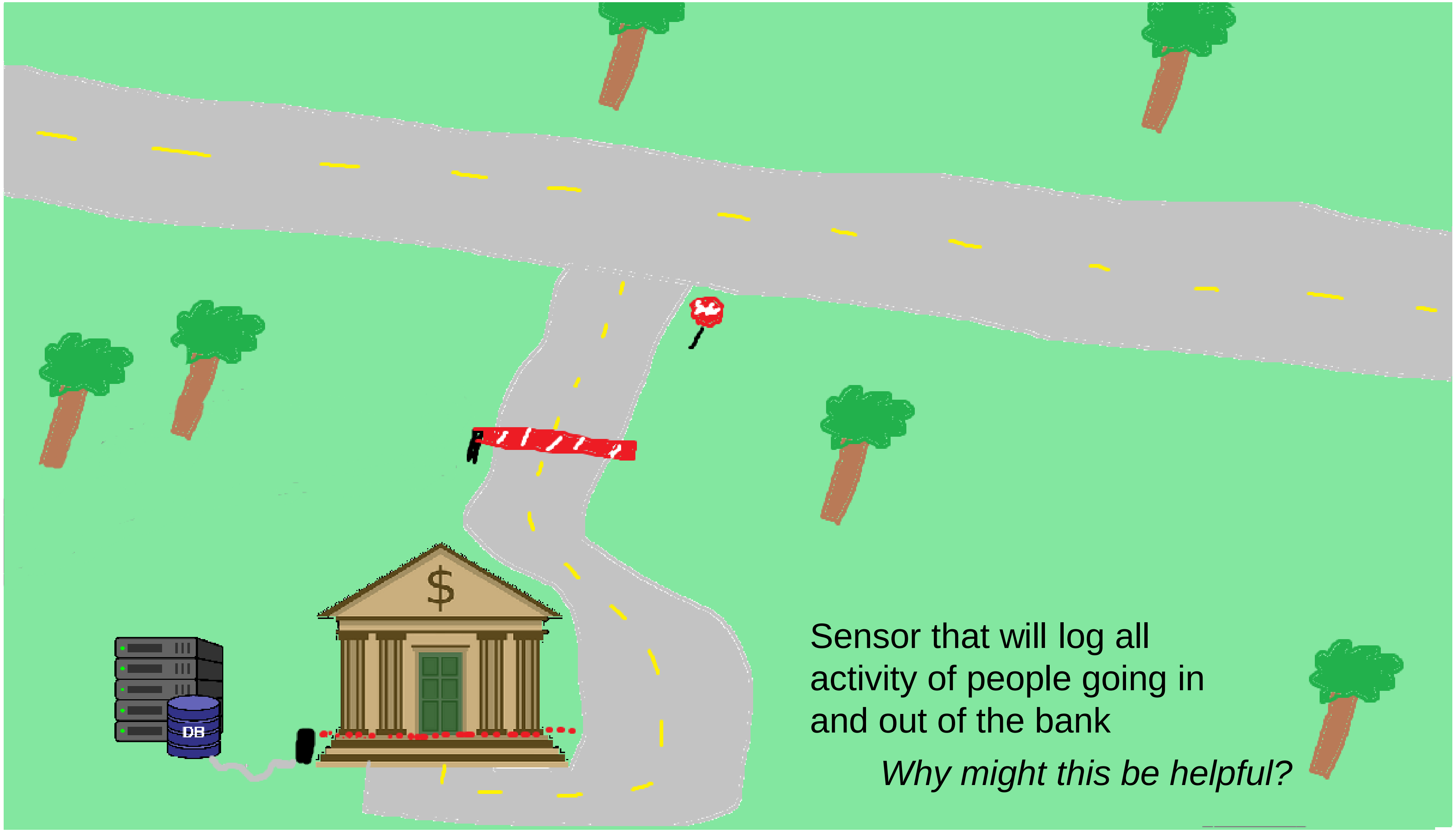


Securing an asset

Humans can be manipulated ☹



Securing an asset

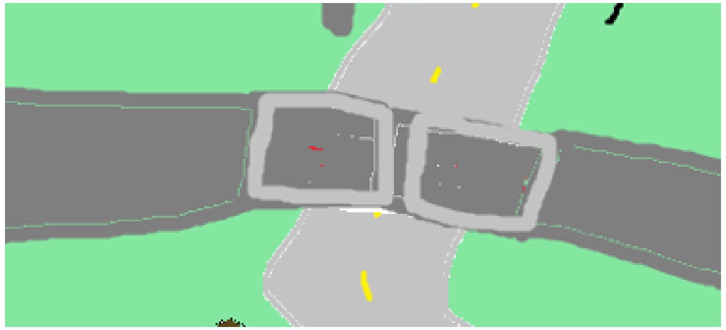


Sensor that will log all activity of people going in and out of the bank

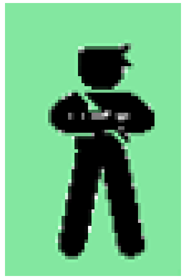
Why might this be helpful?

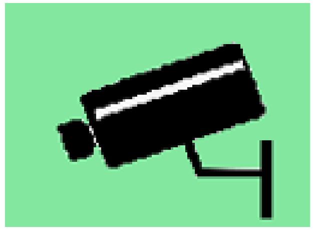
Takeaways

Preventative Security

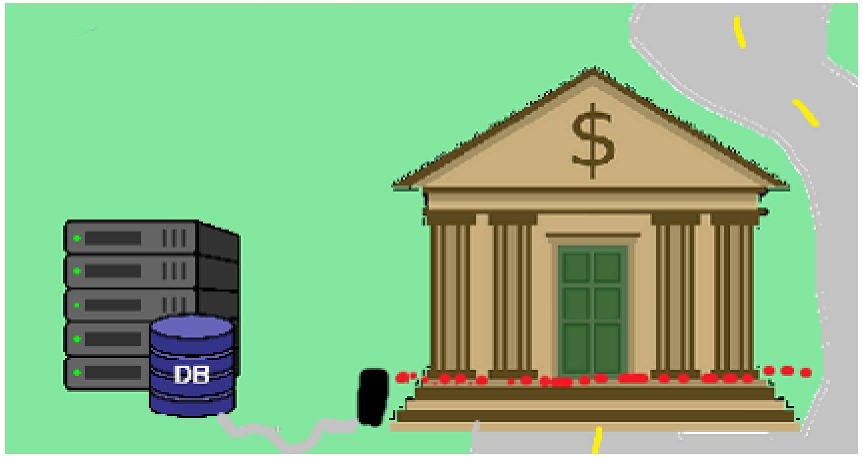


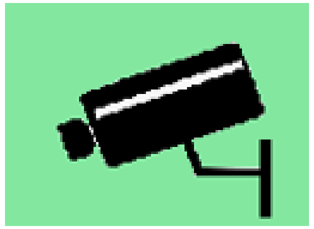
Proactive Security





Logging and Monitoring





CSCI 466- 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

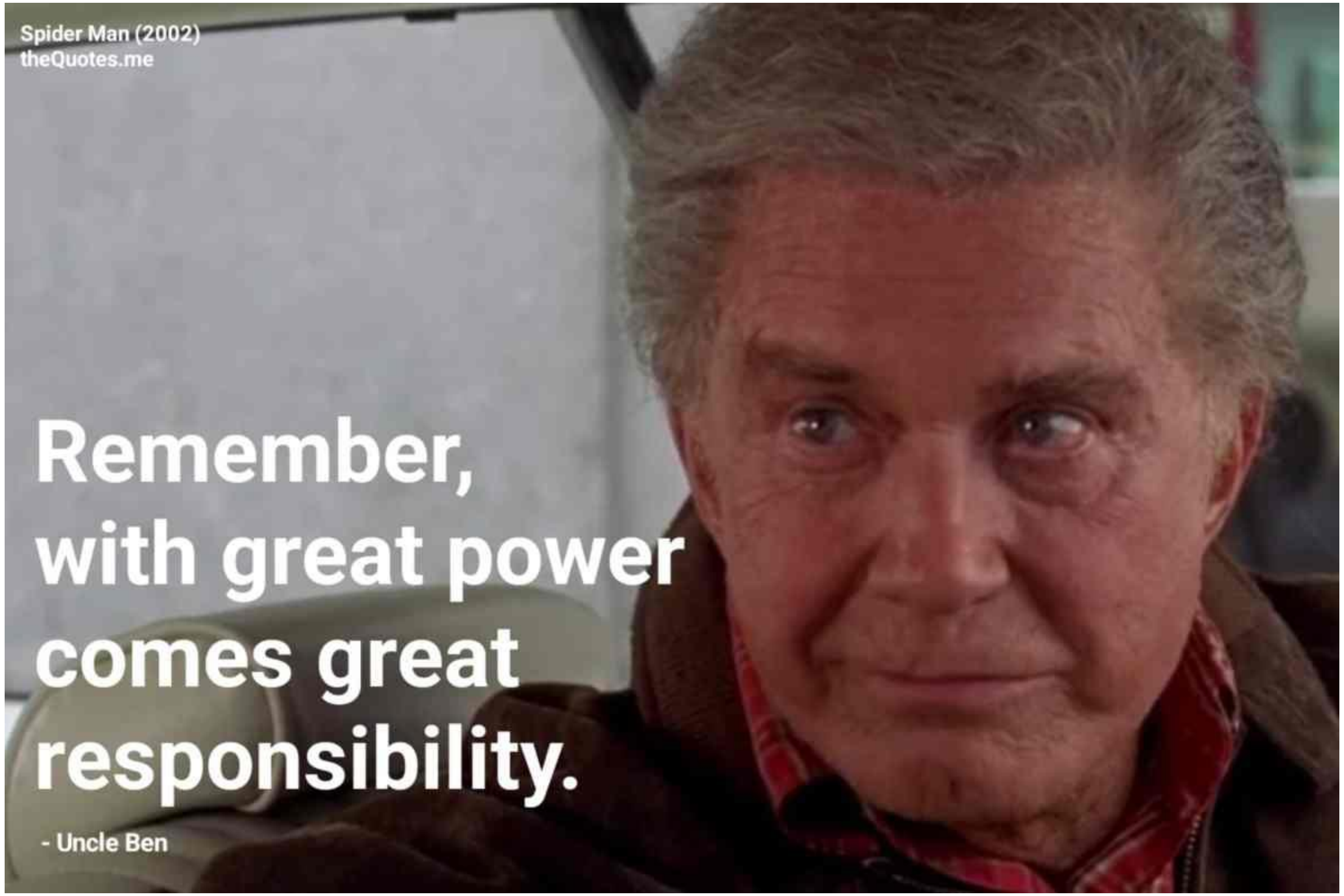
- Understand a variety of relevant vulnerabilities and defenses in **cryptography**

- 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

Kids searching how to hack on Google and accidentally open dev tools
I CAME LOOKING FOR COPPER
AND I FOUND GOLD

(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)

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

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

Hometown
- Billings, MT

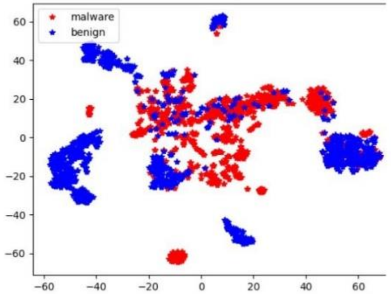
Teaching
- CSCI 466
- CSCI 476

Favorite Cereal
- Frosted Flakes

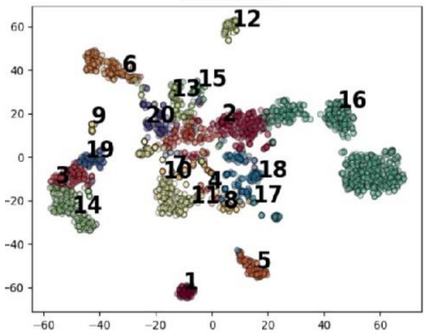
Experience
- Software Engineer and Tester, Techlink (Bozeman)
- Software Engineer, United States Air Force (Hill AFB, Utah)
- Software Engineer, Hoplite Industries (Bozeman)
- Graduate Researcher, MSU (Bozeman)

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

Competitive
Silver 3
62.5 % Win Rate



Kmeans with dim (8)
#clusters = 20



My Experience

This is my first time teaching this class:

Things will not be perfect…

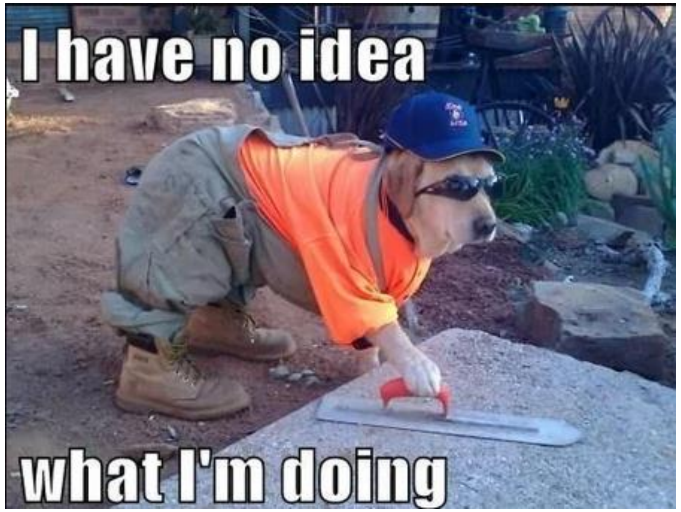
There will be things I don’t know…

I will be stressed…

But I will **always** be on your side, and I want to do whatever it takes to help you succeed!

I appreciate your patience, flexibility, and tolerance

My Experience

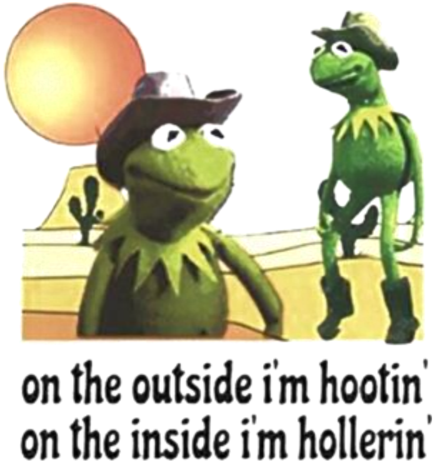


This is my first time teaching this class:

Things will not be perfect…

There will be things I don't know…

I will be stressed…



But I will **always** be on your side, and I want to do whatever it takes to help you succeed!

I appreciate your patience, flexibility, and tolerance

Contact

When you email your professor at 2am and they respond within a minute

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

Office Hours: Monday, Wednesday, Friday 10:00 – 11:00 AM
Thursday 1:00-2:30 PM 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

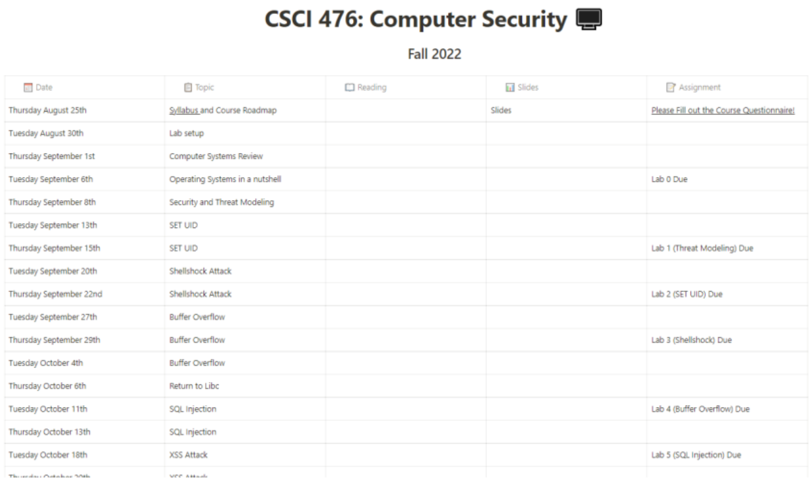
kat hasty
@kathasty

guys really live in apartments like this and don’t see any issue

8:15 PM - 12 Dec 2018

The current state of my office

Logistics



CSCI 476: Computer Security 🖥

Fall 2022

Date	Topic	Reading	Slides	Assignment
Thursday August 25th	Syllabus and Course Roadmap		Slides	Please Fill out the Course Questionnaire!
Tuesday August 30th	Lab setup			
Thursday September 1st	Computer Systems Review			
Tuesday September 6th	Operating Systems in a nutshell			Lab 0 Due
Thursday September 8th	Security and Threat Modeling			
Tuesday September 13th	SET UID			
Thursday September 15th	SET UID			Lab 1 (Threat Modeling) Due
Tuesday September 20th	Shellshock Attack			
Thursday September 22nd	Shellshock Attack			Lab 2 (SET UID) Due
Tuesday September 27th	Buffer Overflow			
Thursday September 29th	Buffer Overflow			Lab 3 (Shellshock) Due
Tuesday October 4th	Buffer Overflow			
Thursday October 6th	Return to Libc			
Tuesday October 11th	SQL Injection			Lab 4 (Buffer Overflow) Due
Thursday October 13th	SQL Injection			
Tuesday October 18th	XSS Attack			Lab 5 (SQL Injection) Due
Thursday October 20th	XSS Attack			

Class Meetings
Tuesday Thursday: 3:05 – 4:20
Reid Hall 102

Course Website: https://www.cs.montana.edu/pearsall/classes/fall2022/476/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

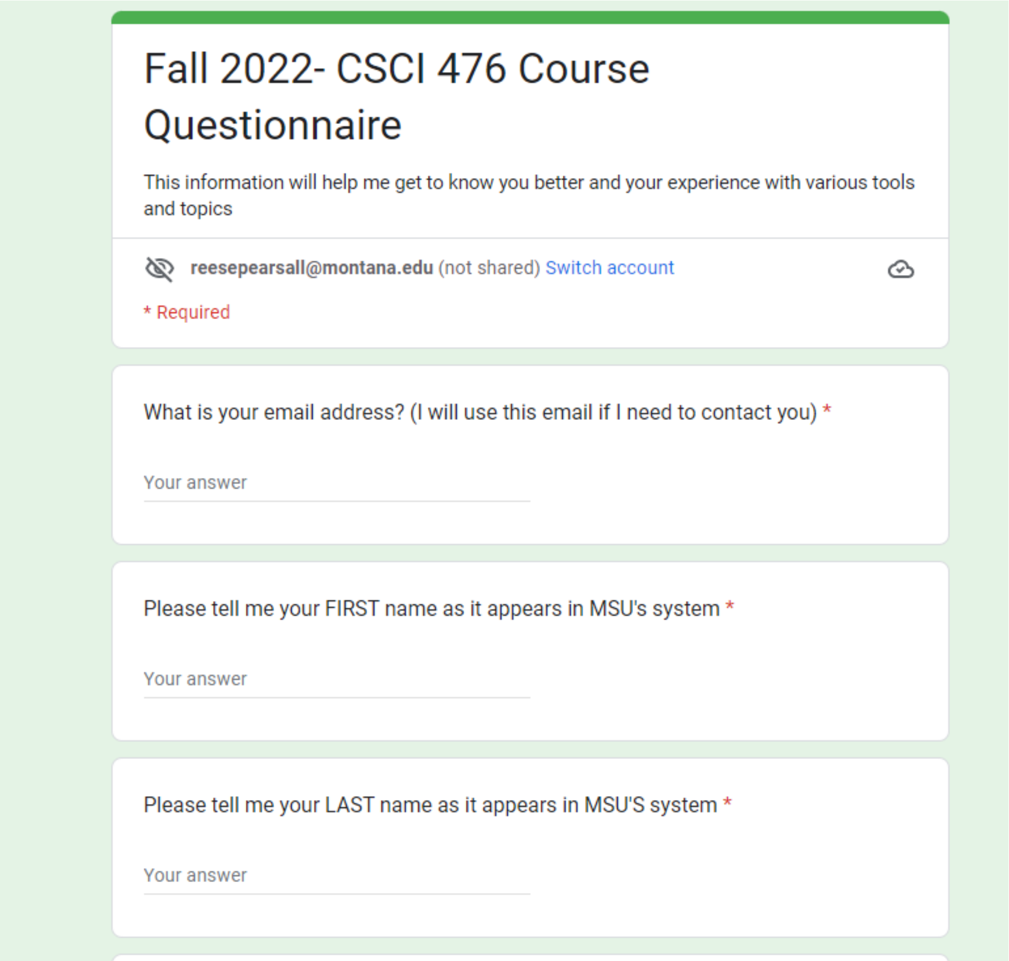
- CSCI 232- Data Structures and Algorithms
- CSCI 366- Computer Systems (recommended)
- CSCI 112- Programming in C (HIGHLY HIGHLY HIGHLY recommended)

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 2022- 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 (not shared) Switch account

* Required

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

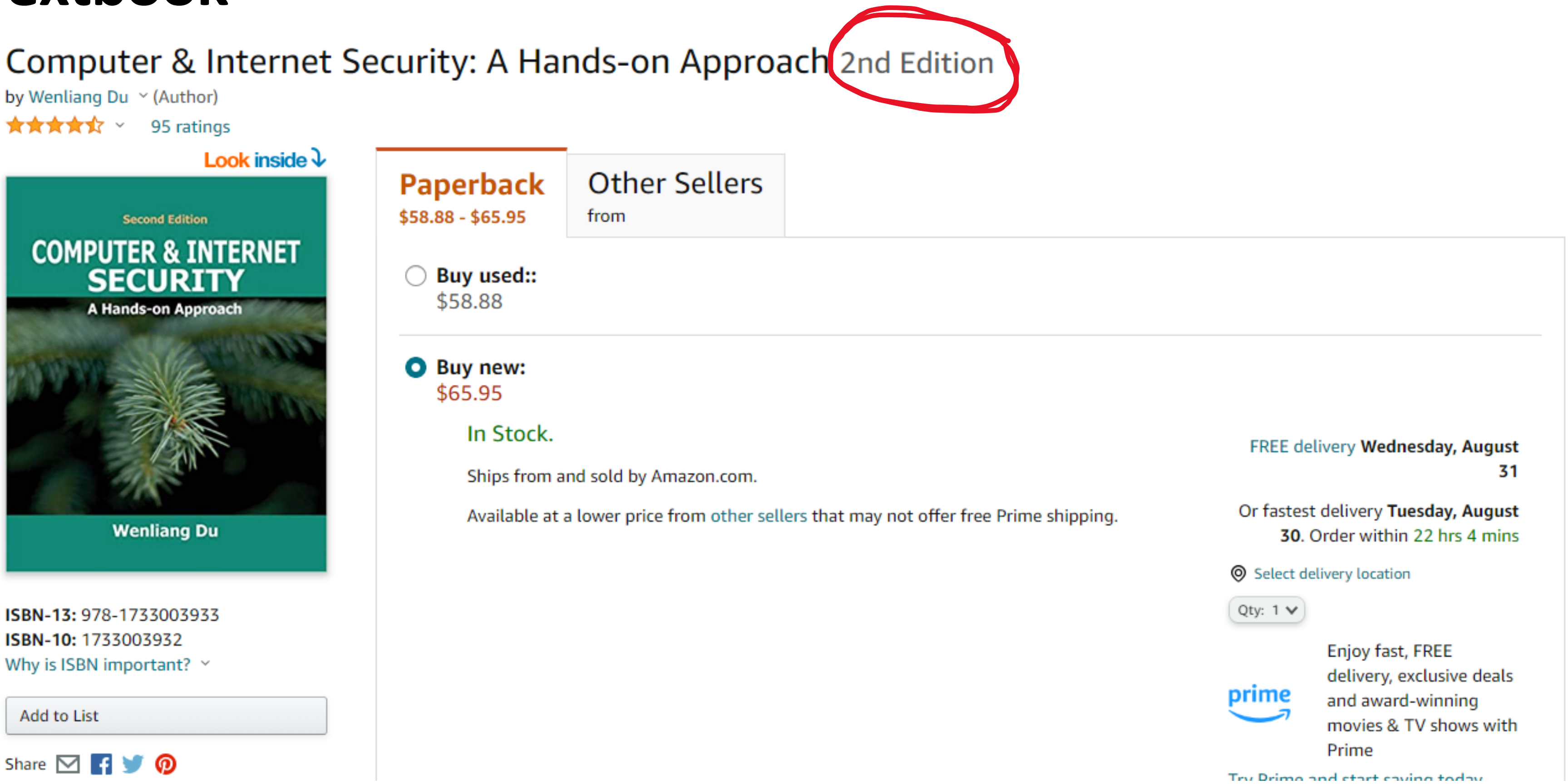
(There seems to be issues with accessing this form while on the MSU network)

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



Computer & Internet Security: A Hands-on Approach 2nd Edition

by Wenliang Du (Author)

★★★★☆ 95 ratings

Look inside

ISBN-13: 978-1733003933
ISBN-10: 1733003932
Why is ISBN important?

Add to List

Share

Paperback
$58.88 - $65.95

Other Sellers
from

○ **Buy used::**
$58.88

● **Buy new:**
$65.95

In Stock.

Ships from and sold by Amazon.com.

Available at a lower price from other sellers that may not offer free Prime shipping.

FREE delivery **Wednesday, August 31**

Or fastest delivery **Tuesday, August 30**. Order within 22 hrs 4 mins

Select delivery location

Qty: 1

prime

Enjoy fast, FREE delivery, exclusive deals and award-winning movies & TV shows with Prime

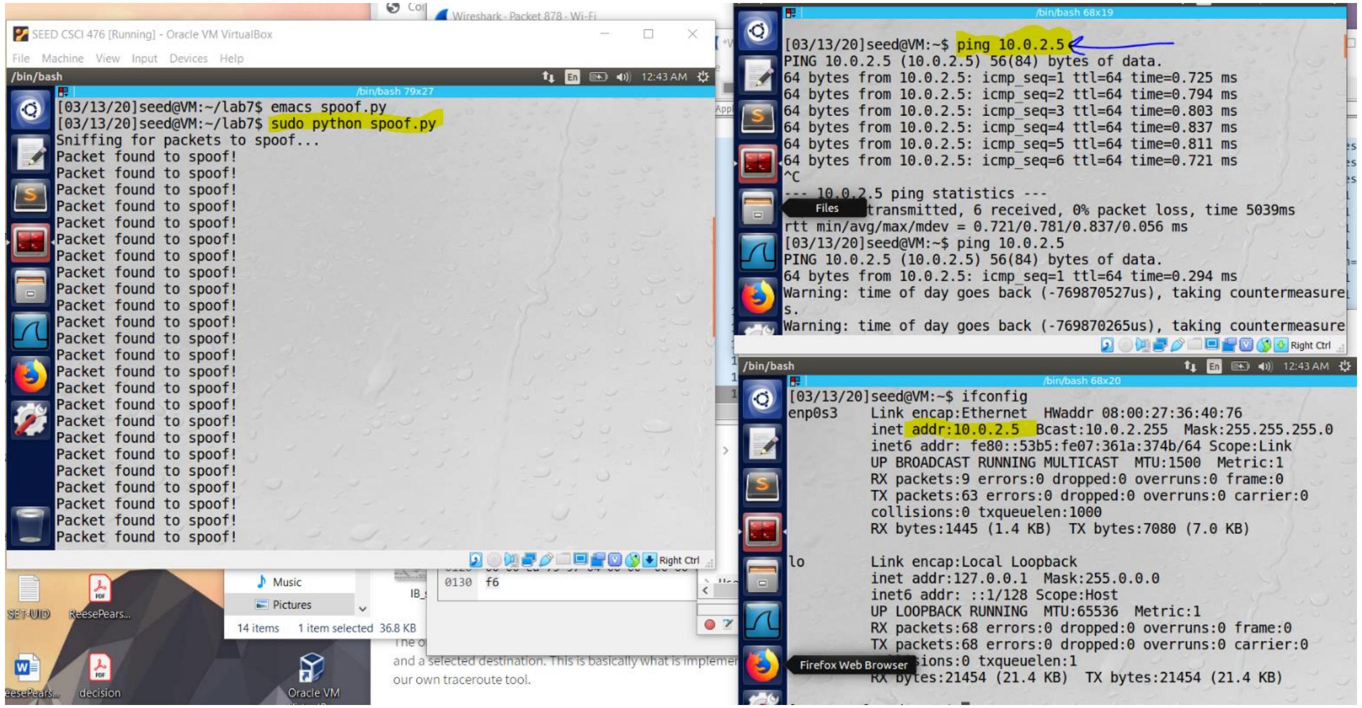
Try Prime and start saving today

- 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

Tuesday will be dedicated to help make sure you have the VM correctly installed (lab 0)

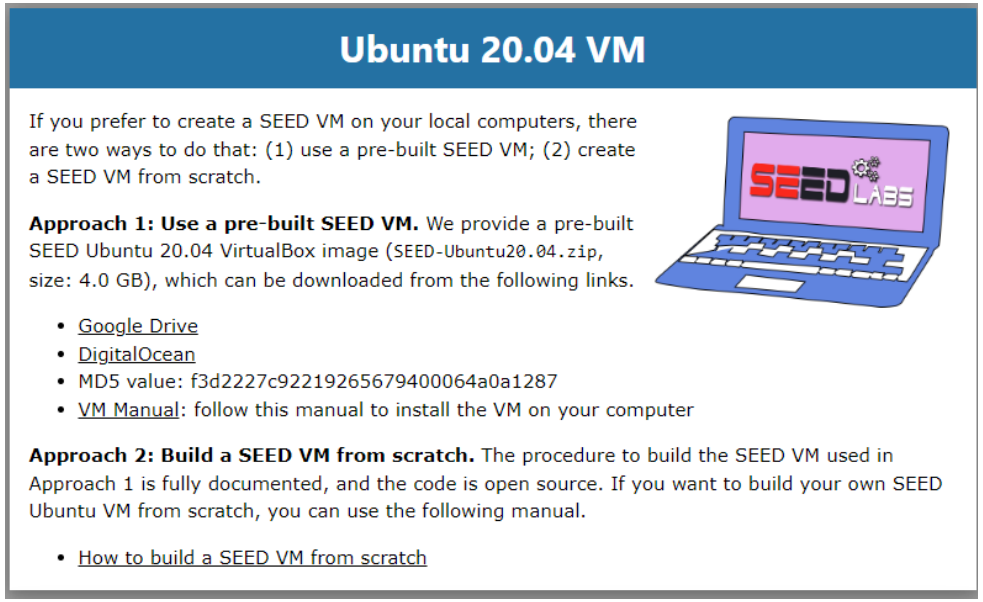


```
[03/13/20]seed@VM:~/lab7$ emacs spoof.py
[03/13/20]seed@VM:~/lab7$ sudo python spoof.py
Sniffing for packets to spoof...
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
Packet found to spoof!
```

```
[03/13/20]seed@VM:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.725 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.794 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.803 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.837 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.811 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=0.721 ms
^C
--- 10.0.2.5 ping statistics ---
         transmitted, 6 received, 0% packet loss, time 5039ms
rtt min/avg/max/mdev = 0.721/0.781/0.837/0.056 ms
[03/13/20]seed@VM:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.294 ms
Warning: time of day goes back (-769870527us), taking countermeasure
s.
Warning: time of day goes back (-769870265us), taking countermeasure
```

```
[03/13/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:36:40:76
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::53b5:fe07:361a:374b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1445 (1.4 KB)  TX bytes:7080 (7.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
             sions:0 txqueuelen:1
          RX bytes:21454 (21.4 KB)  TX bytes:21454 (21.4 KB)
```



Ubuntu 20.04 VM

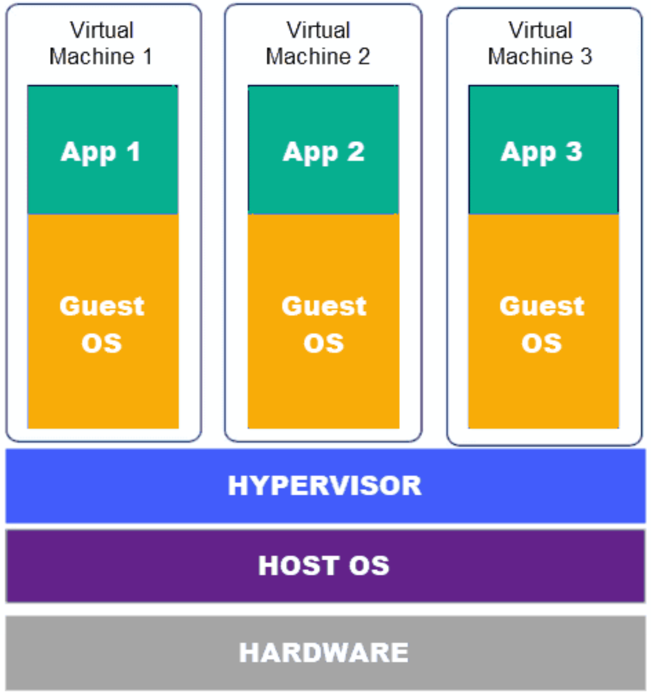
If you prefer to create a SEED VM on your local computers, there are two ways to do that: (1) use a pre-built SEED VM; (2) create a SEED VM from scratch.

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~~ **Final Knowledge Check**

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 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 the last week of classes

- ➢ You must get your topic approved by Reese first

Grading

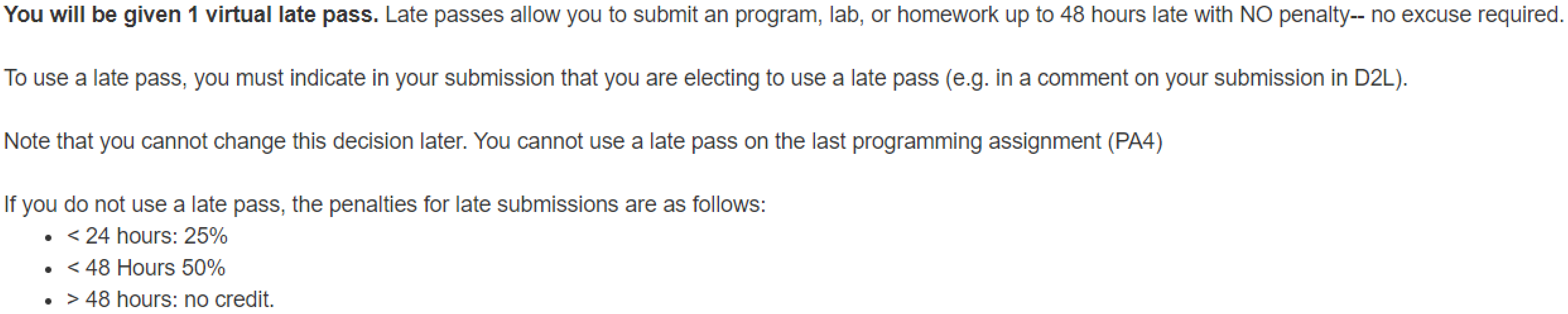
- **15% ~~Final Exam~~ Final Knowledge Check**

➢ Cumulative quiz that evaluates your knowledge of ***important*** topics from the course

➢ Consists of short answer questions

➢ Note sheet is allowed

Late Assignment Policy



You will be given 1 virtual late pass. Late passes allow you to submit an program, lab, or homework up to 48 hours late with NO penalty-- no excuse required.

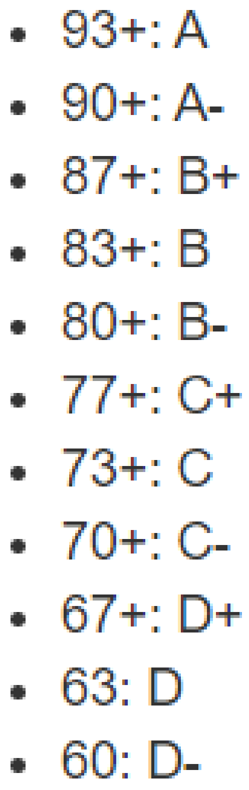
To use a late pass, you must indicate in your submission that you are electing to use a late pass (e.g. in a comment on your submission in D2L).

Note that you cannot change this decision later. You cannot use a late pass on the last programming assignment (PA4)

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

juju 💰
@ihyjuju

in college you gotta get over L’s real quick because the next one is due at 11:59

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?

Lab 0

Activity?