CSE 484 Assignment -- Homework # 1
(Due 2pm October 5 -- no late submissions)

Names of team members:

_____
_____
_____
_____

UWNetIDs of team members:

_____
_____
_____
_____

Group Assignment: You should work in groups of 1 to 4 people (we *strongly* encourage groups of size 2 to 4). You will be divided into the *same groups* for an in-class exercise on Wednesday.

Out: Monday, October 3.

Due: Wednesday, October 5, 2:00pm -- 30 minutes before class. ***No late submissions allowed.*** *We will be doing an exercise during class on Wednesday, October 5 that builds on this assignment and hence this assignment must be submitted on time*.

Obtaining full credit: We expect to give 100% credit to any submission that satisfies all the criteria we describe below -- there are no "right" or "wrong" answers. This primary purpose of this assignment is to help you start *thinking* about security.

How to submit: Catalyst: https://catalyst.uw.edu/collectit/assignment/dhalperi/17513/67740

You can download and edit this Word file directly. *But submit only a PDF file, not a Word file -- we have an automatic script for printing PDF files and will* not *print nor grade Word submissions.*

For class on Wednesday, Oct 5: In addition to submitting your assignment on time, please also bring a printed copy to class on Wednesday (on printed copy per group should be sufficient).

Familiarize yourself with this whole assignment before beginning: Read this assignment in its entirety before you begin.

Background from Lecture 2: You should familiarize yourself with slides 31-35 from Lecture 2: http://www.cs.washington.edu/education/courses/cse484/11au/lectures/Lecture02-Au-2011.pdf. These slides help provide definitions / examples of *assets*, *adversaries*, and *threats*.

How much time to spend: This assignment has two parts -- Part 1 is focused on automotive security and Part 2 is focused on Web mail security.

You should spend at *at least 25 dedicated minutes total* but *at most 35 minutes total* on *each* of Part 1 and Part 2. That means that this assignment should take at least 50 minutes total (for Parts 1 and 2 combined) but at most 70 minutes total (for Parts 1 and 2 combined).

You should spend at least *25 dedicated minutes* (not distracted by other things) on *each* of Part 1 and Part 2 because we want you to not just think about the "obvious" things, but to think a bit more deeply. But we don't want you to spend too much time -- so stop after 35 minutes.

Again, spend between 25 and 35 dedicated minutes on Part 1 and between 25 and 35 dedicated minutes on Part 2.

Start your timers *after* you read this assignment in its entirety. Said another way, you should already be familiar with this assignment and understand the questions herein before you start your 25-35 minute timers.

If you would prefer to work on paper, you may take extra time (beyond the 35 minutes per part) to transcribe your printed notes into a digital document for submission.

Use of the Web and other materials: Since the primary goal of this exercise is to help you to start thinking about security issues, we request that you *not* use external information (the Web, other friends, and so on) while completing this assignment. You should use only the information contained within this document and only talk with your project team members.

Assignment Part 1: Computer Security for the Modern Automobile

Background on automotive computer systems: The modern automobile has become pervasively computerized. In some cars, computers control critical components like the brakes, the engine, the lights, steering, and acceleration. These computers are also connected via internal, wired computer networks within the car. The interconnections between these components dramatically helps improve vehicle safety and efficiency. For example, computers attached to the wheels can detect if one wheel is spinning faster than another -- an indication of a potentially dangerous skid. These wheel speed sensors can send a message to some other computer within the car that can then instruct the brake computer to apply additional brake pressure to the wheel that is spinning too quickly. This sequence of events -- made possible because of within-vehicle computer networks -- is what makes sophisticated safety systems, like traction control, possible.

Many computers within the car also have *wireless* radio interfaces. For example, many cars have Bluetooth hands-free calling. This means that a computer within the car can pair with

a Bluetooth phone, and the driver can use microphones within the car as well as the car's speakers for his/her calls. Modern cars also receive satellite radio signals and GPS radio signals. Many modern cars also have built-in cellphones. These built-in cellular capabilities make it possible for the car to call 911 if it detects an accident, and also make it possible for the car manufacturer to unlock a person's car doors if he/she forgets his/her keys in the car.

Now, spend between 25 and 35 dedicated minutes thinking about and answering the following questions.

Question 1: When considering the design of a modern, computerized automobile, what do you think the *ASSETS* should be? Include as many assets as you can think of, but don't worry if you can only think of a few.

The assets you mention do not need to all be assets to same party. Different actors in the system may have different assets, so make it clear which actors will view these assets as assets.

1.
2.
3.

… (Add more numbers if you wish.)

Question 2: Who do you think the primary *ADVERSARIES* are, and what might the *GOALS* of those adversaries be? Include as many adversaries and their associated goals as you can think of, but don't worry if you can only think of a few.

1.
2.
3.

… (Add more numbers if you wish.)

Question 3: How do you think someone might go about trying to attack the system. That is, what do you think the *THREATS* are? For example, password cracking is a threat against an encrypted filesystem, and a fake voter smartcard is a threat against an electronic voting machine. Include as many threats as you can think of, but don't worry if you can only think of a few.

1.
2.
3.

… (Add more numbers if you wish.)

Question 4: Given all of the above, what do you think are the most important security concerns for the modern automobile?

1.
2.
3.

… (Add more numbers if you wish.)

Question 5: Attestation of time spent:

[ ] Check this box if your group spent at least 25 dedicated minutes on this problem, but no more than 35 minutes.

Assignment Part 2: Web Mail

Background on Web mail systems: Many of you are probably already familiar with Web mail systems -- systems like GMail, Hotmail, Yahoo! mail, and so on. Web mail systems are generally free -- users can go to their preferred service provider and create a Web mail account. They can then access their Web mail account from a browser anywhere around the world, and often from their phones as well. These Web mail systems benefit users, who now have a free email account, and benefit the system providers in various ways that depend on the service providers' business models.

Now, spend between 25 and 35 dedicated minutes thinking about and answering the following questions.

Question 6: When considering the design of a Web mail system, what do you think the *ASSETS* should be? Include as many assets as you can think of, but don't worry if you can only think of a few.

The assets you mention do not need to all be assets to same party. Different actors in the system may have different assets, so make it clear which actors will view these assets as assets.

1.
2.
3.

… (Add more numbers if you wish.)

Question 7: Who do you think the primary *ADVERSARIES* are, and what might the *GOALS* of those adversaries be? Include as many adversaries and their associated goals as you can think of, but don't worry if you can only think of a few.

1.
2.
3.

… (Add more numbers if you wish.)

Question 8: How do you think someone might go about trying to attack the system. That

is, what do you think the *THREATS* are? Include as many threats as you can think of, but don't worry if you can only think of a few.

1.
2.
3.

… (Add more numbers if you wish.)

Question 9: Given all of the above, what do you think are the most important security concerns for Web mail systems?

1.
2.
3.

… (Add more numbers if you wish.)

Question 10: Attestation of time spent:

[ ] Check this box if your group spent at least 25 dedicated minutes on this problem, but no more than 35 minutes.