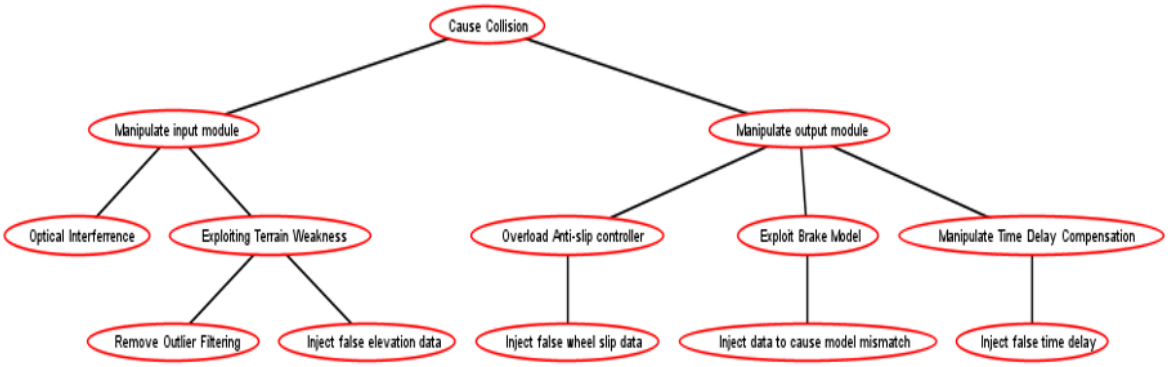
Q1



The above attack tree shows ways to attack the AEB feature of autonomous vehicles which can cause collision.

1. **Manipulating the input module:**

    a) Optical interference - If the LIDAR sensor is blinded by intense sunlight or rain, it may give false readings, activating the AEB system when it's not needed, or it may fail to detect any object that comes in its vicinity (Montalban, n.d.), therefore the AEB system would not be triggered, causing collision.

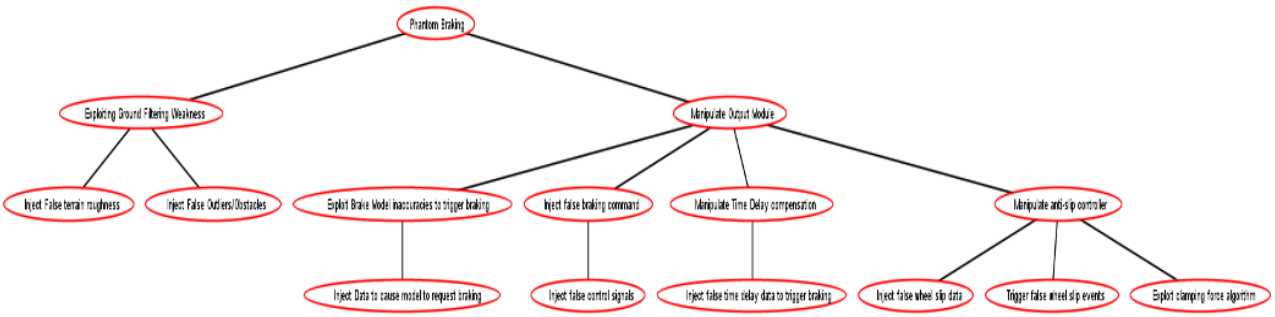
    b) Exploiting terrain map weakness - An autonomous car relies on sensor data and communication devices for input to drive the car (Meng et al., 2010). If we inject false elevation data or remove outlier filtering to exploit terrain map weakness into the car's sensors, the decision support system may make incorrect decisions, causing collision.

2. **Manipulating the output module:**

    a) By injecting false wheel speed data, the attacker can overload the anti-slip controller, causing collision (Yang et al., 2022).

    b) By injecting data to cause model mismatch, the attacker can exploit the brake model - An autonomous car relies on complex software models to control various vehicle functions, including braking. If we inject data to cause a model mismatch, this can lead the braking system to behave in unpredictable ways, causing collision.

    c) By injecting false time delay, the attacker can manipulate time delay compensation - The data provided by the sensors is used to make decisions, such as when to brake. Injecting a false time delay increases the time to activate the AEB, causing collision.



The above attack tree shows ways to attack the AEB feature of autonomous vehicles to cause phantom braking:

1.Exploiting ground filtering weakness - By injecting false terrain roughness data or injecting false outliers, we can cause the system to misinterpret a smooth ground to have an obstacle (Meng et al., 2010), which causes unnecessary braking.

2. **Manipulating output module** -

a) Exploiting brake model inaccuracies to trigger breaking - By injecting false data, we can make the model believe that emergency braking is necessary.

b) Injecting false braking command - We can manipulate the signals that control the brake actuators. By sending false signals, we can directly activate the brakes, regardless of the system's calculations.

c) By Injecting false time delay data - the attacker can manipulate time delay compensation to trigger braking.

d) Manipulating anti-slip controller: An attacker can cause anti-slip controllers to prevent wheel lockup during braking (Yang et al., 2022), leading to phantom braking:

i) By Injecting false wheel slip data - an attacker can confuse the AEB system into thinking that the vehicle is slipping which would lead to unnecessary braking.

ii) Trigger false wheel slip events - By directly manipulating the data from the sensor, the system can be made to think a wheel is slipping (Grove et al., 2020).

iii) Exploiting clamping force algorithm - By manipulating the algorithm we can cause the brakes to apply excessive force.

Q2

CAUSE COLLISION - Using the attack potential parameters I have calculated the attack feasibility of one branch each for the manipulation of Input and output module:

MANIPULATION OF INPUT MODULE (OPTICAL INTERFERENCE)

Attack Potential Parameters	Value Assigned	Rating
Elapsed time	<1 WEEK	0
Specialist Knowledge	PROFICIENT	3
Knowledge of the target	PUBLIC	0
Window of opportunity	EASY	1
Equipment	STANDARD	0

Attack Feasibility	Ratings	Total
High	0+3+0+1+0	4

Optical interference has high attack feasibility, while removing outlier filtering and injecting false elevation data have very low to medium feasibility. Hence, I have chosen this branch to calculate its attack feasibility. It doesn't require a long time to set up as the equipment required to perform the attack should be standard, in case they use lasers or bright flashlights to blind the LIDAR, these equipment are easily available. Knowledge required should be proficient as the attacker should be familiar with the working of optical sensors. Furthermore, data about the working of optical sensors should be publicly available. Window of opportunity should be easy as the attacker can access the sensors without significant effort.

MANIPULATING OUTPUT MODULE (Injecting false time delay)

Attack Potential Parameters	Value Assigned	Rating
Elapsed time	<6 months	4
Specialist Knowledge	EXPERT	6
Knowledge of the target	CONFIDENTIAL	7
Window of opportunity	MODERATE	4
Equipment	SPECIALISED	4

Attack Feasibility	Ratings	Total
VERY LOW	4+6+7+4+4	25

This is a very risky attack that one can perform as it leads to Incorrect Predictions, causing collision. This requires a long time to set up as the equipment required to perform this attack is specialized as the hardware tools required to perform the attack are not readily available, but can be acquired with effort. The expertise required to perform this attack should be expert as the attacker should be familiar with vehicle dynamics, reverse engineering skills, and timing parameters, which should be confidential information. I have assigned the window of opportunity to be moderate as it requires access to the vehicle's internal communication network.

PHANTOM BRAKING – Using the attack potential parameters I have calculated the attack feasibility of one branch each for the manipulation of Input and output module:

INJECTING FALSE TERRAIN ROUGHNESS

Attack Potential Parameters	Value Assigned	Rating
Elapsed time	<6 months	4
Specialist Knowledge	EXPERT	6
Knowledge of the target	CONFIDENTIAL	7
Window of opportunity	MODERATE	4
Equipment	SPECIALISED	4

Attack Feasibility	Ratings	Total
VERY LOW	4+6+7+4+4	25

Within exploiting ground filtering weakness, I have focused on injecting false terrain roughness. This should take time to execute because to perform this attack, the attacker will require specialized tools such as CAN bus interfaces. The attacker should need expert expertise to execute this attack as they should be familiar with specific algorithms to interpret terrain roughness. Data about AEB algorithms and terrain roughness is confidential information. I have assigned the window of opportunity to be moderate as the attacker might need access to the vehicle's internal network, which is not easily available.

INJECTING FALSE WHEEL SLIP DATA

Attack Potential Parameters	Value Assigned	Rating

Elapsed time	**<6 months**	**4**
Specialist Knowledge	**EXPERT**	**6**
Knowledge of the target	**CONFIDENTIAL**	**7**
Window of opportunity	**MODERATE**	**4**
Equipment	**SPECIALISED**	**4**

Attack Feasibility	**Ratings**	**Total**
VERY LOW	**4+6+7+4+4**	**25**

Injecting false wheel slip data affects the anti-slip controller's ability to prevent the wheel from slipping. This should take time to execute as the attacker would need specialized tools, such as CAN bus interface is required to perform this attack. The attacker should need expert expertise to execute this attack as they should be familiar with communication protocols to transmit data. Information about calculation of wheel slip data algorithms should be confidential information. I have assigned the window of opportunity to be moderate, as injecting false wheel slip data should require physical access, which should be limited.

Q3

Asset	Compromised property	Casual chain	Adverse consequence	Stakeholders
ESR	Integrity	Spoofing leading to False Distance/Speed detection	AEB fails to detect objects accurately causing collision or phantom breaking	Pedestrians, people in the vehicle, people behind the vehicle
LIDAR	Integrity	Data manipulation causing detection of false obstacle	False braking causing collision or phantom breaking	Pedestrians, people in the vehicle, people behind the vehicle
ESP	Integrity, availability	Injecting malicious commands causing brake failure.	AEB's fails to control the vehicle's braking causing collision or phantom breaking	Pedestrians, people in the vehicle, people behind the vehicle

HMI	Integrity	Spoofing causing False Warning messages.	Driver takes unnecessary action or ignores genuine warnings causing collision or phantom breaking	Pedestrians, people in the vehicle, people behind the vehicle

ESR (Electronic Scanning Radar) - An input module that plays an important role in the AEB system as it detects the presence of objects in the vicinity of the vehicle. Compromising the integrity of ESR data can have severe consequences as it may lead to collisions if the radar cannot detect an object in front of it, or leads to phantom braking if it assumes an object is there but in reality, it's not.

Lidar (Light Detection and Ranging) - Another input module that plays an important role in the AEB system as it is used for object detection**.** LIDAR is not as efficient for close-range or intensive object detection tasks, such as collision resistance during parking or bumper protection (Hussain & Zeadally, 2019). It helps in decision making, hence its integrity is very crucial. Incorrect data from LIDAR can cause collisions.

ESP (Electronic Stability Program)- An output module that plays an important role in the AEB system as it controls the braking system of a vehicle. If ESP'S integrity or availability is compromised, this can lead to AEB failing to control the vehicle's braking, causing collision.

HMI (Human-Machine Interface)- Another output module that plays an important role in the AEB system as it interacts with the driver, delivering information such as warnings of collision threats. If the HMI's integrity is compromised, it can lead to the driver getting false warnings about potential collisions or not sending warnings at all, causing collisions with an obstacle or a vehicle behind it.

References:

Grove, K., Camden, M. C., Krum, A., Hanowski, R. J., & Virginia Tech Transportation Institute. Center for Truck and Bus Safety. (2020). *Research and Testing to Accelerate Voluntary Adoption of Automatic Emergency Braking (AEB) on Commercial Vehicles* (No. FMCSA-RRT-18-013). https://rosap.ntl.bts.gov/view/dot/49335

Hussain, R., & Zeadally, S. (2019). Autonomous Cars: Research Results, Issues, and Future Challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1275–1313. https://doi.org/10.1109/COMST.2018.2869360

Meng, X., Currit, N., & Zhao, K. (2010). Ground Filtering Algorithms for Airborne LiDAR Data: A Review of Critical Issues. *Remote Sensing*, *2*(3), Article 3. https://doi.org/10.3390/rs2030833

Montalban, K. (n.d.). *Advancing LiDAR perception in degraded visual environments: A probabilistic approach for degradation analysis and in inference of visibility*.

Yang, Y., Liu, Y., & Wang, C. (2022). Development and Validation of AEBS Anti-slip Control Model for In-wheel Motor Drive EV in AMESim Co-simulation with Matlab/Simulink. *Journal of Physics: Conference Series*, *2219*(1), 012013. https://doi.org/10.1088/1742-6596/2219/1/012013