Solve the Sleigh's CAN-D-BUS Problem

So, Santa suspects **The Lollipop Gang** is attacking his infrastructure, and that his sleigh appears to have been hacked. Coincidence, or the work of the same attackers?

Objective

Jack Frost is somehow inserting malicious messages onto the sleigh's CAN-D bus. We need you to exclude the malicious messages and no others to fix the sleigh. Visit the NetWars room on the roof and talk to Wunorse Openslae for hints.

Difficulty: 3/5

Wunorse Openslae's dialog:

Say, do you have any thoughts on what might fix Santa's sleigh? Turns out: Santa's sleigh uses a variation of CAN bus that we call CAN-D bus. And there's something naughty going on in that CAN-D bus. The brakes seem to shudder when I put some pressure on them, and the doors are acting oddly. I'm pretty sure we need to filter out naughty CAN-D-ID codes. There might even be some valid IDs with invalid data bytes. For security reasons, only Santa is allowed access to the sled and its CAN-D bus. I'll hit him up next time he's nearby. Hey Santa! Those tweaks you made to the sled just don't seem right to me.

I can't figure out what's wrong, but maybe you can check it out to fix it.

Hints

Chris Elgee is talking about how CAN traffic works right now!

Solution

Note

It's helpful to complete the CAN-BUS Investigation terminal before attempting this objective.

CAN Bus is a communication bus designed to allow vehicle microcontrollers and computers to communicate without using a host computer. Devices on the bus communicate via messages that are received by every device on the bus. A

rogue or misconfigured device on the bus can cause a vehicle to malfunction. Someone is inserting malicuous messages on the CAN-D bus on Santa's sleigh. From Wunorse's dialog, it appears we need to fix 3 things:

- 1. The brakes shudder when applied.
- 2. The doors are acting oddly.
- 3. Some valid IDs have invalid data.

Using the interface to the CAN-D Bus in the sleigh, we can see the current traffic on the bus. We can simulate the major functions on the sleigh: starting & stopping the engine, locking & locking the doors, and applying the accelerator & brakes.

	ID: EPOCH TIME ID MESSAGE
Accelerator: 0	16098 13066369 O 19#00000000
Accelerator.	Comparison Operator: 16098 13066574 188#0000000
	Equals 16098 13066574 244#000000000
Brake: 0	Message Criterion: 15038 13055575 080#000000
	Exclude 16038 13066384 188#0000000
Steering: 0	ID Operator Criterion Remove 15098 13055984 244#000000000
	16038 1306hoh8 080#000000
	16098 13067 178 C 19#0000000
Start	16098 13067393 188#0000000
	16098 13067393 244#000000000
	16038 13067483 080#000000
Stop	16098 13067583 C 19#CCCCCCCC
	16038 13067803 188#0000000
Lock	
Unlock	

A good starting point is to filter out the "noisy" traffic that's making it difficult to find the malicious messages:

	ID:						EPOEH	TIME	ID MESSAGE	
Accelerator: 0							16098	H35306 (198#000000F2057	
		Со	mparis	son Op	erator:		16098	1433 (603	198#000000F2057	
		Eq	Juals		-		16098	143365-18	198#000000F2057	
Brake: 0	Message Criterion							14338865	198#000000F2057	
bruke. o	00	00	00	00	00	00	16098	14340-103	198#000000F2057	
			E	clude			16098	14340604	198#00000000000	
Steering: 0		Operator	Crite	rion		Remove	16098	14342 (68	198#00000F000000	
Steering. 0	188		Citt				16098	143447 18	198#000000F2057	
	019	All				ē	16098	143474 19	198#000000F2057	
Start	244						16098	14352084	198#000000F2057	
Juli	080	All					16098	14363453	198#000000F2057	
							16098	14366523	198#000000F2050	
Stop							15098	1430 1325	198#000000E2050	
Stop							15098	14305350	198#000000E2050	
	/						16090	14308952	198#000000F2050	
Lock		1 1					15090	14383830	198#000000F2050	
LOCK					_			יירטכטטיי	100#0000000000000000000000000000000000	
		1						בו רו סכרו מככססכטו	130#000000C031	
Listade								000000	100#0000000000000000000000000000000000	
υπίοςκ			мах				16038	19330-185	198#000000FC05'i	
							16038	19903353	198#000000F2051	

By process of elimination, we can determinations on what IDs correspond to what function:

- 080 : Brakes
- 188 : Tachometer (RPM gauge)
- 019 : Steering
- 244 : Accelerator pedal
- 19B: Locking mechanism (Lock/Unlock)

Filtering out all traffic from IDs 188, 019, 244, and 080 eliminates all the noisy traffic, and allows us to see that there are messages from ID 19B. There appear to be malicious messages on the bus with ID 19B, so can apply a filter to exclude those messages: ID = 19B:000000F2057.

	ID:						EPOEH	TIME	10 MESSAGE	
Accelerator: 0							16098	1569887 (188#00000000	
		Co	mpai	rison Ope	erator:		16098	15698876	244#0000003F0	3
		Ec	quals		÷		16098	(\$69928.)	188#00000000	
Brake: 0		Ν	/ lessa	age Crite	rion:		16098	15699283	244#0000003F	1
	00	00	00	00	00	00	16098	15699690	188#0000000	
				Exclude			16098	15699690	244#0000003F	1
Steering: -50	ID	Operator	Cr	iterion		Remove	16098	IS100 100	188#0000000	
Ŭ	19B	Equals	00	00000F20	57	•	16098	IS100 100	244#0000003F	1
	080	All					16098	IS100401	188#00000000	
Start	019 All 🗧						16098	IS11008 (6	188#0000000	
	188	All				•	16098	ISAD 1556	188#0000000	
							16098	ISAD 1606	188#0000000	
Stop							16098	15/102046	188#0000000	
							16098	IS7024 IB	188#0000000	
							16098	ISN02861	188#0000000	
Lock							16098	ISA0338 (188#0000000	
	1-						16098	IS703684	188#0000000	
	-		-)			16098	IS7104093	188#0000000	
Unlock							16098	15/10/4503	188#0000000	
		RPM Reinder for Minder					16098	IS1049 (3	188#0000000	
					(

Removing the filter for ID 080 will allow us to look at the oddly-acting brakes. Applying the brakes to 100, we can see messages of 080:000064 (100 in base 10), but also some errant messages with ID 080 but values > FFFFF0.

			ID:		EPOEH	TIME	ID MESSAGE
Accelerator: 0		080			16098	16438899	080#000064
		Com	parison Operator:		16098	16438904	OBD#FFFFFR
		All	-		16098	16439299	080#000064
Brake: 100		Me	ssage Criterion:		16098	16439350	OBO#FFFFF3
			5		16098	16439736	080#000064
			Exclude		16098	16439838	OBC#FFFFB
Steering: 0	ID	Operator	Criterion	Remove	16098	16440323	080#000064
oteening. o	188	All			16098	16440342	080#FFFFF0
	244	All		•	16098	16440843	080#000064
Start	019 19B	All Equals	000000F2057	- 2	16098	16440849	080#FFFFF8
Scare					16098	1644 (353	080#000064
					16098	1644 (355	080#FFFFFD
Stop					16098	1644 1858	080#000064
Jeop					16098	1644 1860	080#FFFFFR
					16098	16442302	080#000064
Lock					16098	16442302	OBC#FFFFG
LUCK					16098	16442882	080#000064
	-	1			16038	16442882	OBD#FFFFFD
					15098	16443292	080#000064
OHIOCK		RPM MAX			15098	16443309	

We can apply a filter for ID 080, values containing FFFFF to eliminate the misbehaving brakes. This last filter fixes Santa's sleigh and solves the objective.

	EDOSINE ID MESSAGE
Accelerator: 0	Sleigh deFrosted! 302909 080#000000
	Comparison Operator: 16098 1700296 1 0 19#0000000
	Equals - 16098 17003062 188#0000000
Brake: 0	Message Criterion: 16098 17003 165 244#000000000
	Exclude 16098 17003469 0 19#0000000
Steering: 0	ID Operator Criterion Remove 15098 17003569 188#0000000
	080 Contains FFFFF • 15058 17003830 244#000000000
Start	
C 1	
Stop	
LOCK	
UNIOCK	
	עוועעעעראיי בכפרעעויי פבעפו

Answer

Correctly filter the CAN-D Bus traffic to eliminate the problems with the sleigh.