Security measures in DRIVERLESS CARS

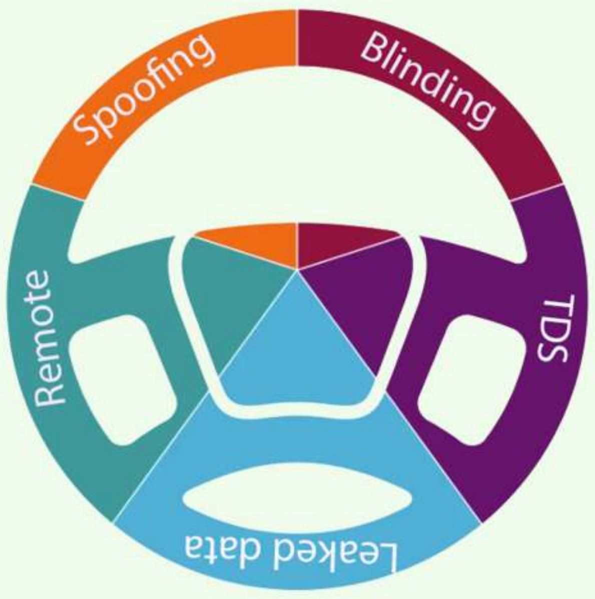
Rameez Hussain

Cybersecurity threats

Jamming is caused by overloading the car receivers with noise, signals, and messages that cause interference. A car communication system can be prevented from receiving messages by sending out a signal of larger power on the same frequency. **Replay attacks** rely on attacking the lidar by creating fake echoes making real objects appear closer.

Blinding the car radar system by jamming the RF signal using signal generators. Attackers can disable onboard cameras using lasers or can perform blocking attacks. Blinding relies on open wireless communication, blocking the car receiving GPS or GNSS signals.

Spoofing attack tricks sensors, cameras, and receivers with invalid information. Sending fake messages, warnings signals to change the behaviour of the car. A threat on the lidar using low power lasers or pulse generators in tricking them into slowing down and fooling driving sensors etc. Ultrasonic and parking sensors can be fooled into seeing non-existent objects.



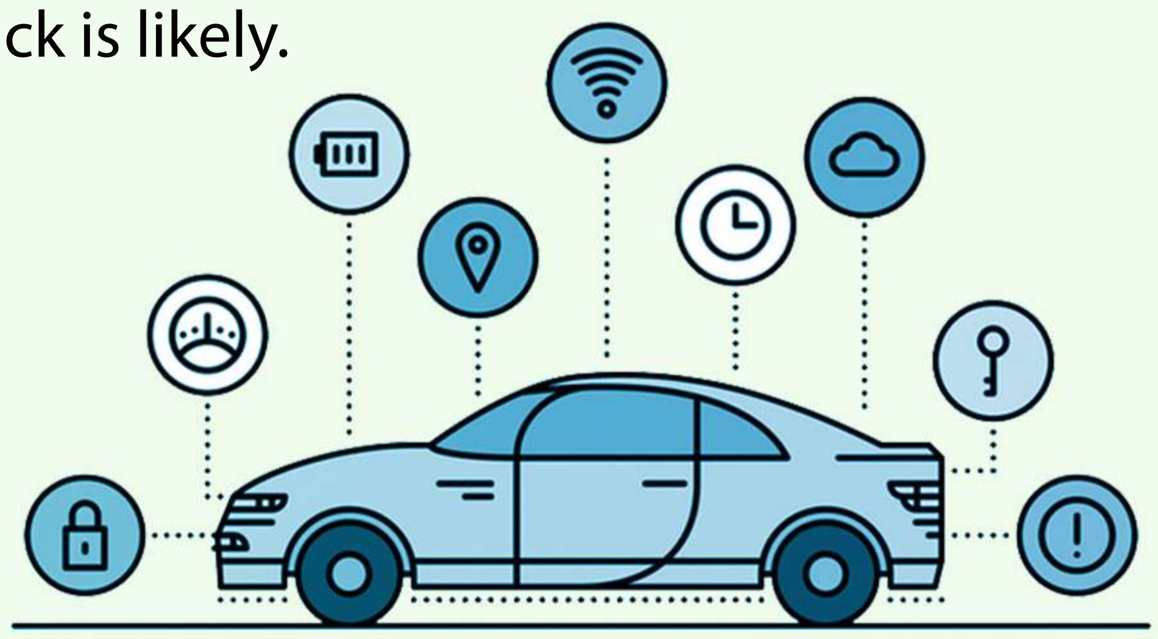
Time delay switched attack is when an attacker inserts a time delay into a networked control system. In driverless cars, this affects the critical imminence in which the controllers receive information affecting sensor function and leading to accidents.

Solutions to such threats

Driverless cars have been equipped with **emergency** braking, lane recognition, and parking assist features.

Counter-interference measures, data authentication, encryption and sender-car identification requirements are put into place against jamming and spoofing attacks such as weakening the car communication system.

The car communication system will only accept **authorised communication,** and **safety protocols** enabling the car to go into lockdown mode when an attack is likely.



Disabling car software; when a spoofing attack takes place, the passenger can avoid this functionality by using the steering wheel and pedals to pull over safely.

GPS and GNSS signals should make sure that they are using **cryptographic authentication signatures** in protecting against spoofing attacks.

Remote access system including diagnostic unit should include **cryptographically** secure entity authentication techniques.

Issues in the future

- Agreeing on cryptographic methods for vehicle communication system.

- Unauthorized commands send to electrical core units.

- Securing entity authentication techniques

- Vehicle ad hoc networks should be redesigned

References

Intranet.royalholloway.ac.uk. (2019). [online] Available at :https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2016/computer-weekly-articles/michaelhaddrellcw.pdf [Accessed 6 May 2019].

Medium. (2019). 5 Key Challenges faced by Self-driving cars. [online]Available at: https://medium.com/@ritidass29/5-key-challenges-faced-by-self-driving-cars-ed04e969301e [Accessed 1 May 2019].