Autonomous Vehicle Safety

Vincent W. S. Chan

IoT/Smart City is a new paradigm and not merely a linear extension of the past Internet. It provides basic services as well as innovative services that can enrich human life. However, the security challenges will be huge due to the large number of deployed devices, open interfaces and possibilities of insider attacks. Currently, there is inadequate consideration of the security aspect of the Smart City network and urgent attention is required. This article will look at Smart City security from the perspective of autonomous vehicle safety.

Smart Cities will soon have driverless cars in many cities mixed with traditional transportation. Autonomous vehicles will redefine how objects and people move from place to place and will soon become a significant part of the future global infrastructure. Safety should be the primary concern for such a system. A good commonly accepted principle for security and resiliency of any complex system is that "the system is only as safe as its weakest subsystem". The exception are systems that are specifically designed to use unreliable components and systems. One extreme example is a Byzantine robust network where network assets are assumed to be compromised, but if there is at least one surviving path between source and destination, the Byzantine network protocol will eventually find that path and deliver the message. With the numerous attack surfaces of 5G (and many new ones beyond 4G) and its lack of proven and verifiable security, autonomous vehicle safety cannot solely depend on the Smart City network.

Autonomous vehicles like many systems can break down in hardware or software, fail their mission and even cause harm to occupants and pedestrians. The current generation of automobiles already has automatic messaging and limited software updates via open air wireless interfaces. My 2019 vehicle has that feature and several months ago the electronic control unit displayed an "immediate software service required" directive. I would have stopped using the vehicle until a dealer could fix the software. Fortunately, I had a car computer with software specific to the vehicle and was able to reset some trivial "fault" codes brought on by the recent updates without the trouble of going to a dealer. Last week I received a new directive from the manufacturer of my handheld car specific computer that I need a software update to deal with the car's new ECU software. On the one hand, I am grateful for the responsiveness of the car manufacturer on updating the software in my car and the diagnostic computer manufacturer advising me to update my software to deal with the changes. On the other hand, this confirms that no system is perfect and periodic updates are required and the ease of software changes is a cause for alarm. The SolarWinds breach is a rude awakening example of how software updates may be exploited for harm. A casual search on the Internet will find incidents of breach for most auto manufacturers' car computers.

Benign failures apart, the numerous vulnerabilities can be exploited for nefarious purposes. While we have yet to see a major coordinated terrorist attack employing autonomous vehicles, we cannot be complacent. As they become even more ubiquitous and integrated in our lives, their vulnerabilities will surely be exploited for harm and social disruption. Autonomous vehicles can be hacked from remote locations. Perpetrators are difficult to track down, especially if they act at a distance and through bots. Thus, for pragmatic reasons, autonomous vehicles and also conventional automobiles must have at least two modes of safeguards. The first mode of operation depends on the Smart City network for guidance and navigation (connected autonomy); in the second mode, the vehicle itself must have sensors and computers isolated from the outside network (isolated autonomy) that provide safeguards such as emergency braking, collision avoidance and speed control.

Having a huge number of objects on the Smart City network substantively increases the risks of external and insider attacks and there can be a constant presence of compromised nodes. A new security paradigm that allows good operations in the presence of compromised nodes and constant insider attacks must be adopted as a major shift from previous assumed models. Vehicle safety is an extreme example; communication between vehicles and roadside units about local road information must be accurate and timely. For driverless cars, the threats of denial-of-service or jamming attacks are of particular concern. If the large data network is to play a critical role in the guidance and navigation of automobiles, the integrity of link state data will be important for time deadline limited vehicular control and management functions. With the growth of SDN (software defined networks) and NFV (network function virtualization), control plane security becomes very critical. If learning algorithms are used in support of network operations, then data contamination can be especially dangerous, impacting not only immediate actions, but also future decisions. There is no time horizon for deployment of a verifiably secure Smart City network that we can let human lives depend on. While we can try every effort to secure that network, the vehicle must have a second isolated autonomy mode where its own sensors and computers can provide basic safeguards without external inputs, and also at the same time the hardware and software are isolated from the influence of the outside infrastructure network. At this point there are no vehicles that can provide this isolated autonomy, and the Smart City network is not nearly secure enough. Those who advocate for deploying autonomous vehicles now are playing with fire and irresponsible. Breaching of an automobile's computer is not a hypothetical event but has happened repeatedly. Much research and development is needed to provide adequate safeguards. Since there is a time deadline issue for sensing and control (as fast as ~10mS), cyber security techniques that typically react in seconds or even minutes will not work for this application. Layered defenses that are often used in high quality security systems may also not be available because of the need for low complexity, low delay open air interfaces and networking.

Government and manufacturers must collaborate on stimulating and conducting R&D to deter avoidable tragedy by developing frameworks, architectures, and standards to mitigate risks, and they must prepare for the consequences of misuse and attacks using autonomous vehicular technology. While R&D should be left to the professionals in the private sector, government must play a vital role in the leadership of developing safety standards much like what they have done for seatbelts and other physical safety standards. We should not wait for a major catastrophe to wake us up!