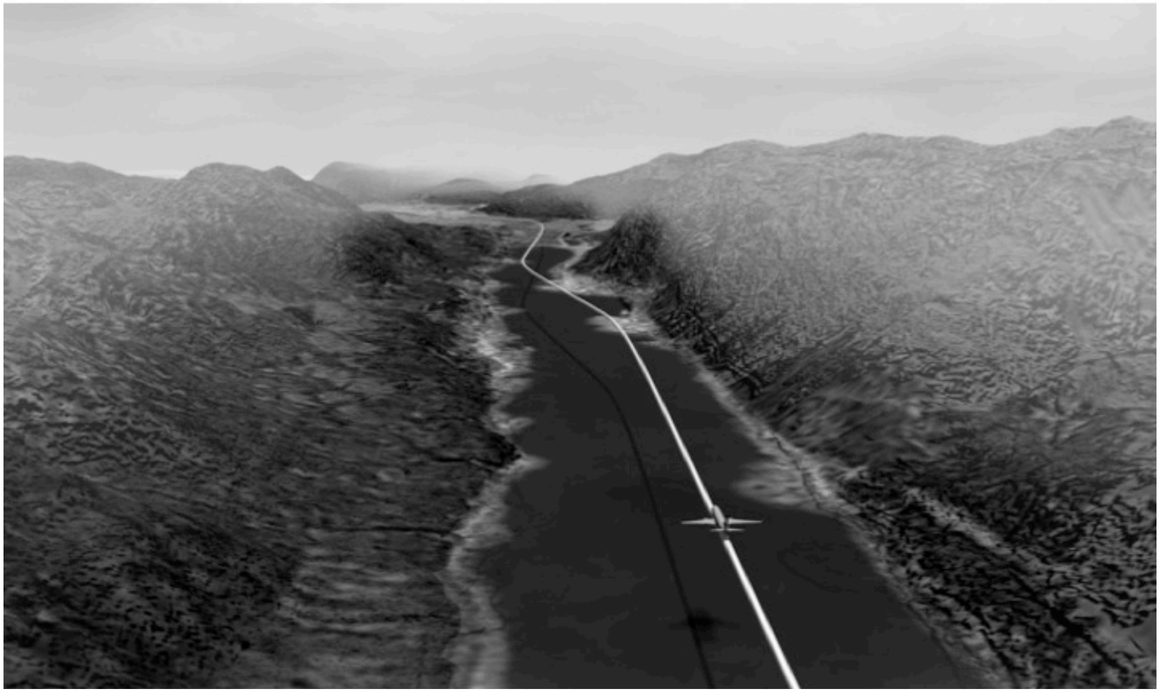
Cyber Safety for Transportation

by Per Enge, March 9, 2015

Prologue: Today, pilots bound for Juneau follow the twisting Gastineau Channel shown in Figure 1, which shows the capital city of our northernmost state at the end of this channel. On a clear day, our pilots enjoy the beautiful mountains in the Alaskan panhandle. On a dark and stormy night, they rely on satellite navigation to guide their aircraft down this now forbidding fjord. Specifically, they rely on the navigation system to warn them within a few seconds if the location error may be larger than one hundred meters. They count on the residual risk to be lower than one approach per ten million.

Figure 1: Approach to Juneau Airport



Tomorrow, automatic vehicles will descend from the air and populate our roadways (automatic driving assistance systems or ADAS), railways (positive train control, PTC) and waterways (ships without crews). Moreover, the sky will be filled with aircraft that carry no pilots to mitigate flight risk. These will be drones or un-piloted air vehicles (UAVs). For efficiency, cars will drive while the enclosed humans snooze or send texts. Trains will slow and speed certain that they alone occupy the underlying track. Drones will fly confidently between buildings to monitor air pollution and crime in our major cites. All told, the benefit will be great.

Why must we protect this new world of transportation? Cyber terrorists, e-criminals and hackers will also shift their gaze. They will now ply their trades on the mobile transactions between these new driverless vehicles rather than rack-bound computers. They will use jammers to deny guidance at the worst of times; they will use spoofers to misdirect the driving machines; and eavesdropping to steal sensitive information.

Senator Markey (D-Massachusetts) has sounded the alarm. His propitious report, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, asks the right questions.

> "Can hackers gain access and hijack some of these essential functions?
> Can information on driver location be used for commercial purposes without the driver's knowledge or consent?"

In short, he is concerned about both security and privacy, and his survey finds nearly all new cars are vulnerable to such intrusions.

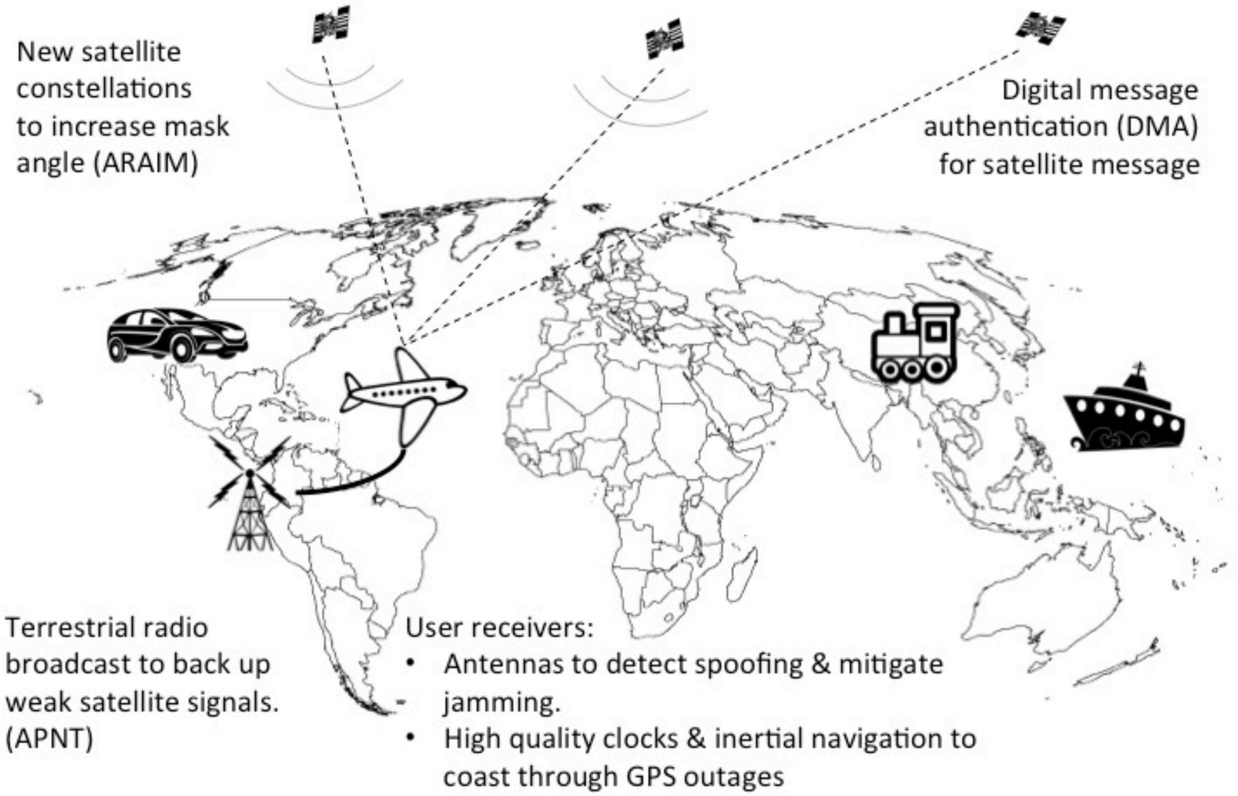
Sophisticated navigation systems will guide the vehicles of our autonomous future, but navigation frailty has already been demonstrated. For example, researchers from the University of Texas hijacked the GPS signals used to navigate a yacht in the Mediterranean Sea. This was a cooperative demonstration, but made the frightening point that ill-intentioned people could control ship guidance. Counterfeit GPS signals have also been used to capture the navigation of a drone over White Sands testing range. See Humphreys, 2014. These are so-called spoofing attacks where the authentic signals are replaced with counterfeits and the misdirection occurs without the driver's knowledge. They are complicated, but very dangerous.

Jamming attacks are more prevalent than spoofing attacks. They are commonplace and simple: they use strong radio signals to overwhelm (jam) the radio signals used for navigation and surveillance. Such attacks are not artful; they do not introduce misdirection; they simply deny the guidance service. For example, people carry personal jammers to protect their privacy when they do not want to be tracked. Such personal privacy devices knocked out GPS operations at Newark's Liberty Airport for several months before analysts discovered trucks on the New Jersey turnpike carried them to prevent tracking. A priest has also deployed a radio jammer to knock out cell phone calls during his sermons, and this transmitter also knocked out GPS.

Finally, data theft is also a threat. Markey found that most new automobiles do report data that can be stolen and understood by ill-intentioned parties. His staff found that automobile manufacturers collect large amounts of driving history and vehicle performance data. Often this data is given to third party data centers, and no effective means to secure this stored data is provided. Moreover, no data retention policy exists across the industry. Customer awareness is low, and customers cannot conveniently opt out.

What must we do? Cyber safety for transportation will not be solved with one stroke of the pen or keyboard. It will require legal elements to discourage jamming and spoofing. It will require social protocols that convey the inappropriateness of such dangerous activities. It will require technical work to toughen GPS receivers with new satellite signals, digital message authentication, intelligent antennas and inertial sensors. Safety against jammers and spoofers will also require us to augment GPS navigation with completely independent sources of time and location; perhaps these diverse sources will be placed in low earth orbit or make use of terrestrial transmitters. Figure 2 shows these technical items.

Figure 2: Cyber safety will require many technical advances.


New satellite constellations to increase mask angle (ARAIM)
Digital message authentication (DMA) for satellite message
Terrestrial radio broadcast to back up weak satellite signals. (APNT)
User receivers:
• Antennas to detect spoofing & mitigate jamming.
• High quality clocks & inertial navigation to coast through GPS outages

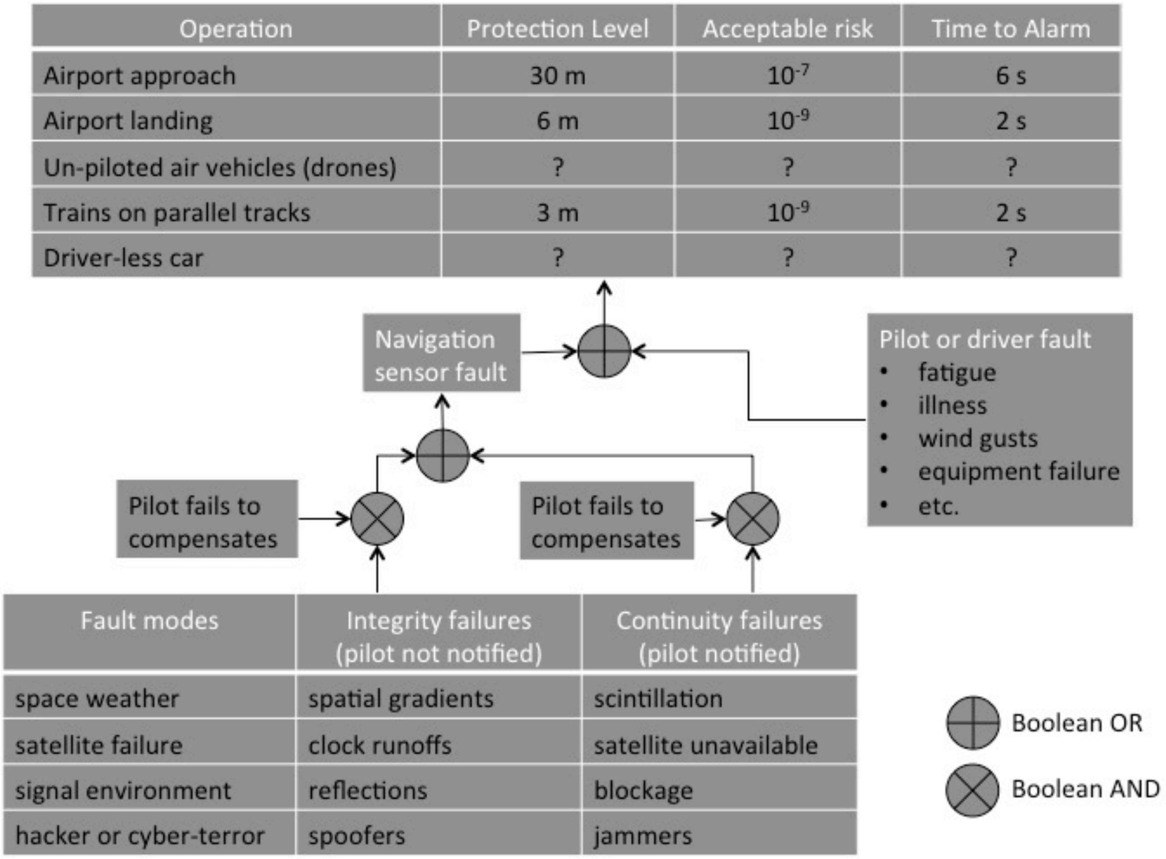
Who will do this work? The needed research begins with the early Stanford actors that have already started this work. They include Professors Boneh (CS), Lee (EE), Hollberg (Physics), Kochenderfer (AA), Enge (AA) and Dr. Walter (AA). These people have begun to craft the pieces shown in Figure 2. They have worked to design a secure signature system based on cryptography to authenticate the digital portion of the information from GNSS satellites. Their students have designed new antennas that are small and can discriminate between satellite signals and potential jammers. Their laboratories focus on clocks and time-transfer techniques that will augment or even supplant GPS. They have deployed un-piloted helicopters that hunt GPS jammers.

However, our present proposal transcends our current faculty. New blood is needed to broaden the bridges between Aeronautics & Astronautics, Computer Science, Applied Physics and Electrical Engineering. These new people must also build bridges to the disciplines of Law, Business, Political Science and Biology.

Time frame, success measures: Securing our new transportation infrastructure will take 30 years. Success will be clearly marked: navigation and surveillance systems will no longer be the object of frequent attack. In fact, they will be so strong that they can be used to secure other systems. In other words, our effort will first lead to security *for* location and then it will reach security *from* location. In the intermediate period, products in the marketplace will indicate progress. Some of these products will be developed with federal funding and others will come entirely from the industrial sector.

Why at Stanford? Stanford is ideally positioned to foster cyber-safety for transportation, because we encourage work across disciplines. Figure 3 is a fault tree and provides another view of our go forward plan. The top of the diagram shows the target level of safety for a variety of canonical transportation operations ranging from aircraft landings to train control. The lower portion of the fault tree shows the fault modes that may propagate upwards and threaten this safety target. As shown, our challenge is intrinsically multi-disciplinary. Multiple modes of transportation are at risk; and the threats arise from all corners of our physical world.

Figure 3: Fault tree for navigation safety



Operation	Protection Level	Acceptable risk	Time to Alarm
Airport approach	30 m	10^{-7}	6 s
Airport landing	6 m	10^{-9}	2 s
Un-piloted air vehicles (drones)	?	?	?
Trains on parallel tracks	3 m	10^{-9}	2 s
Driver-less car	?	?	?

Fault modes	Integrity failures (pilot not notified)	Continuity failures (pilot notified)
space weather	spatial gradients	scintillation
satellite failure	clock runoffs	satellite unavailable
signal environment	reflections	blockage
hacker or cyber-terror	spoofers	jammers