Securing the Future of Transportation

Ulf Lindqvist
SRI International
333 Ravenswood Ave, Menlo Park, CA 94025
ulf.lindqvist@sri.com
Phone 650-859-2351

There is general agreement that safety is a very important aspect of transportation, and we find safety among the primary goals driving the development of cyber-physical systems (CPS) for ground and air transportation. The assumption is that a computer system is much more likely to make timely and correct decisions than a human, and therefore safety is increased when a human driver is supported by a computer system or the vehicle is autonomously controlled by a computer without a human in the loop. However, if we cannot ensure a high level of *security* for the CPS in connected and autonomous vehicles – that is, protecting them from intentional cyberattacks – then we cannot ensure a high level of safety either. Therefore, safety is dependent on security, making security a topic of significant importance for transportation CPS.

Experience in IT systems has shown that we regrettably cannot rely on the goodhearted nature of everyone on the Internet as an approach to system security. There are many types of potential attackers, ranging from young "script kiddies" to organized criminals or even nation states, and their objectives vary accordingly. With large numbers of both automated indiscriminate attacks and sophisticated targeted attacks happening daily on the Internet, we need to protect transportation CPS regardless of whether we are able to predict all types of threats to those systems. While attacks on IT systems can have severe economic consequences, for transportation CPS the potential loss in terms of human lives and health as a result of a cyberattack means that we must do a much better job at security CPS than we are currently doing with IT systems.

There are many challenges and unsolved problems in the field of cybersecurity in general – see for example [1] and [2]. Cybersecurity for CPS poses additional challenges (see for example [3]) not least due to the potentially severe consequences of an attack, and there are yet additional cybersecurity challenges that are specific to transportation CPS. Here, we briefly outline some of those specific challenges and propose some research directions to begin to address them.

Generally speaking, in a research agenda, there are some fundamental questions that the agenda needs to answer:

- Where are we today?
  - What is the current technology and research?
  - What are the important technology gaps and research problems?
- Where do we want to be X years from today?
  - What will solutions look like?
  - What will the solutions enable us to do?
- What will it take to get us there?
  - How can we divide the problem space?

    - What can be done in the short, medium, and long term?
    - What resources are needed?
- How will we know that we got there?
    - How should we evaluate technologies and validate results?
    - What are the metrics of success?

Those questions cannot all be answered for cybersecurity in transportation CPS within the limits of this brief position paper, but we can start to outline a vision of where the field needs to go so that the transportation systems of the future can be safe and secure.

First, let's look at the primary mode of individual transportation – the automobile. There is no question that cybersecurity is a significant issue for automobiles, as the "connected car" concept is becoming reality, and there are more and more computing and communication systems in regular cars – see for example [4] and [5]. In the U.S., a consumer can compare and learn about vehicle safety by reviewing 5-star crash test ratings, recalls, and other safety information from the National Highway Traffic Safety Administration (NHTSA, www.safercar.gov). However, when it comes to cybersecurity, there is no way for consumers to compare the level of security of one automobile model to another, and there is not even any established way for experts to do so. Consumers have no way to make informed decisions, and they cannot choose a modern car that is not computerized and wirelessly connected, because such cars are no longer being manufactured. Research is needed to develop meaningful **metrics** to accurately measure the security of the vehicle as a system, including but not limited to processes for development and integration of components, system design and implementation, and realistic security assessment and exploratory penetration testing. Metrics are also needed to determine the impact on security of any system changes, including any added security mechanisms, so that we can tell whether a given change will raise the security level to the desired extent or if it will have an undesired impact such as lowering the security level. ***Vision:*** *By the year 2020, all new automobiles on the consumer market will go through a mandatory comprehensive cybersecurity assessment with a resulting rating similar to the 5-star crash rating system.*

Because the development of CPS used in automobiles is feature-driven, just like the development of general-purpose IT systems, we know that vulnerabilities will be repeatedly introduced – it is simply the nature of fast-paced development where features and not security is the top priority. It is therefore important that the CPS has strong robustness and resilience properties, so that vulnerabilities and the attacks that exploit them are limited in scope and effect. An attack that successfully penetrates or disables a system component should not be able to easily propagate to other components, as the system should be able to detect the attack, isolate it, and limit its impact. How to achieve this kind of **self-healing** or **intrusion tolerance** in a CPS that has all the constraints of an on-board system in a consumer-market automobile is an open research challenge. It includes aspects of designing and implementing with verifiable security properties, and developing and integrating automated attack detection, diagnosis, and response. ***Vision:*** *By the year 2025, there are automobiles on the consumer market with a built-in transparent capability to automatically detect and safely react to any cyberattacks against its on-board systems.*

In other forms of transportation where CPS are heavily used but not directly owned and operated by individual consumers, such as in rail and aviation, we also face cybersecurity challenges. Given the proclivity of terrorists to attack mass transit, one can imagine scenarios where cyberattacks on CPS could intentionally threaten the safety of large numbers of people. While there are similarities between transportation CPS and the CPS that are industrial control systems (ICS), the fact that transportation CPS platforms are mobile brings particular challenges with respect to attack detection and mitigation. Safety systems can shut down ICS in a manufacturing plant or oil refinery in a fail-safe manner, at potentially high economic cost for the operation but with no safety consequences. When the CPS platform is an aircraft flying at cruising altitude, it is less clear what a **safe system shutdown** would look like from the perspective of the hundreds of people on board. A CPS must be able to maintain safety, as defined by its particular application, even when it is under cyberattack. ***Vision:*** *By the year 2020, all safety requirements and certifications of rail and aviation CPS include stringent cybersecurity metrics and assessments.*

The challenges and visions suggested here are examples of the kind of topics we need to discuss and reach some agreement around, so that we can begin outlining the research path required to ensure that future transportation CPS provide not only more convenience and efficiency, but also improved safety and security.

References

[1] "A Roadmap for Cybersecurity Research." U.S. Department of Homeland Security, Science and Technology Directorate, November 2009. https://www.dhs.gov/csd-resources

[2] "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program." Executive Office of the President, National Science and Technology Council, December 2011.

[3] "Workshop on Future Directions in Cyber-Physical Systems Security." Final Report, U.S. Department of Homeland Security, Science and Technology Directorate, January 2010.

[4] Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In USENIX Security Symposium. 2011. http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf

[5] Miller, Charlie and Valasek, Chris. "Adventures in Automotive Networks and Control Units." August 2013, http://illmatics.com/car_hacking.pdf