Title: Security and Privacy for Cyber-Physical Systems [*This is an original research proposal.*]
Keywords: cyber-physical systems; security; privacy; automobiles; embedded systems

In 2008, a Polish teenager hacked into a city's tram system, derailing four trams [1]. The tram is an example of a cyber-physical system (CPS) in which the computational and physical components are tightly integrated. Increasingly, these systems permeate the world around us. Both NSF and the President's Council of Advisors on Science and Technology [2] have identified cyber-physical systems as a challenge for the future and a priority for national security. NSF Assistant Director Jeannette Wing cited examples spanning multiple fields, such as automobiles, medical devices, ubiquitous sensors, robots, and assistive technologies [3]. Most current CPS are embedded systems, but the trend is towards more full-fledged systems that are networks of interacting elements. As such systems are increasingly integrated into our lives, it is crucial to consider the security and privacy implications: our lives quite literally depend on the security and reliability of these systems. These considerations must be systematically incorporated into their designs; the hacking of the tram demonstrates that weaknesses can and will be exploited. My research will aim to address these issues.

Because CPS is such a broad space, a practical strategy is to study one example and to generalize the results to others. I intend to first focus on the automobile, one of the most widely used CPS today. Modern cars consist of numerous components that are networked together within the car, with many features under direct computer control. While there has been research into security for Vehicular Ad-Hoc Networks (VANETs) [4], which provide communication among vehicles, there has been no systematic focus on the security concerns associated with vehicles themselves. Yet there are networks *within* vehicles, and these networks are becoming increasingly complex. All of a car's components communicate via a specialized internal communications network called a *bus*; as of 2008, all cars sold in the U.S. must implement the Controller Area Network (CAN) bus (ISO 11898). This bus allows communication with almost all of a car's critical components, including the body controller, the engine, the transmission, the brakes, the airbags, the theft deterrent system, and others. Without a security/privacy conscious framework to design new cyber-physical vehicles, future threats will be addressed only in an ad-hoc fashion after they arise, as we see today with personal computing and the Internet.

While one might speculate on the potential weaknesses of today's vehicles, a rigorous experimental foundation is needed to understand the issues and to allow us to enable security in the future. Thus, conforming to the standard process for developing security foundations for new technologies, my research plan consists of both (1) the experimental analysis of an automobile, and (2) the use of this knowledge to improve and enable future security. To facilitate this work, my advisor, Professor Tadayoshi Kohno, has recently obtained a 2009 Chevrolet Impala. We gathered preliminary experimental results with CAN packets sent by a laptop plugged into the car's On-Board Diagnostic (OBD-II) port. Identifying which packets to send is done through a combination of reverse-engineering, observation, and fuzz testing. Results include disabling the engine, locking brakes, increasing the RPM, and manipulating lights, locks, wipers, instruments, sensor readings, and more; this indicates that systematic attacks on all of the car's components are feasible. In a full-blown attack scenario, this may be done to many vehicles at once.

Although my preliminary analysis has already uncovered a number of challenges to securing CPS like automobiles, many questions remain. To fully understand the problem space and the risks, I must deepen my analysis of vulnerabilities in today's vehicles. Beyond continuing to map out what can be done with each component once an attacker has access to the car's network, I will explore potential attack vectors that might provide such access. It is clear that an attacker with physical access to the car may install a malicious component that connects

to the CAN. The nature of such a component is a subject for further research. More potent is the idea of attacks that are possible without physical access to the car. In such a scenario, an attacker might gain network access via short-range wireless, as used by the keyless entry system, or via long-range wireless, as used by cars with OnStar units.

I will then develop a rigorous foundation to ensure security in cyber-physical vehicles through defensive mechanisms. The preliminary experimental results already suggest fundamental problems with the design of car networks: a broadcast bus with access to every component, coupled with insufficient component security and protocols that simply fail under attack. There are several defensive directions that I will explore in my research. One approach might be to augment the existing CAN-sniffing tool to detect abnormal or malicious activity on the network, and to respond by giving a warning alert or taking defensive action. Here it will be necessary to explore the tradeoff between preventing and correcting malicious actions: if rigorous prevention is too expensive, perhaps a quick reversal is sufficient in some cases. Since a redesign of the network will not benefit existing cars, perhaps it is possible to design an add-on for critical components that acts as a packet filter or firewall. This add-on may provide additional benefits, like the ability to add cryptography to validate certain critical packets. Building on these defenses, it will be desirable to design more secure networks and protocols for future vehicles.

The University of Washington is well-suited for these research interests. My advisor, Professor Kohno, has done substantial work on embedded and cyber-physical systems security, including security and privacy for implantable medical devices and for robots. My previous research experience in computer architecture gives me a firm understanding of the layer below these embedded CPS; this knowledge, combined with my experience with security and privacy issues at Amazon.com, uniquely positions me to have a high impact in this space.

Intellectual Merit: Securing cyber-physical systems is fundamentally challenging. Others have shown that CPS as critical as implantable defibrillators can be vulnerable to compromise [5], and my own preliminary research shows that it is possible for an attacker to compromise critical components within a car. Today's CPS do not provide sufficient security because doing so is fundamentally challenging, due to resource constraints, device heterogeneity, the need for compatibility with existing standards, conflicting goals, and the large range of areas spanned by CPS. My research is focused on overcoming these challenges, thereby providing a foundation for securing the CPS of today and tomorrow.

Broader Impacts: There are certainly reasons for securing automobiles themselves. But by studying automobiles, we can also develop a generalized understanding of broader solutions and directions for securing other types of cyber-physical systems. As a nation, we are becoming more dependent on CPS in many critical sectors. This research will provide a foundation for securing future systems, thereby helping to ensure the safety and security of the United States and its citizens. I will also incorporate outreach with K-12 students to help make this age group secure users of technology and to broaden participation in CS (see personal statement).

References:

[1] G. Baker. Schoolboy Hacks into City's Tram System. *Telegraph.co.uk*, Jan. 2008.

[2] PCAST. Leadership Under Challenge: Info. Tech. R&D in a Competitive World, Aug. 2009.

[3] J. Wing. Looking Ahead in NSF CISE. *2009 Computing Leadership Summit*, Feb. 2009.

[4] B. Parno, A. Perrig. Challenges in Securing Vehicular Networks. In *Fourth Workshop on Hot Topics in Networks*, November 2005.

[5] D. Halperin, T.S. Heydt-Benjamin, *et al*. Pacemakers & Implantable Cardiac Defibrillators: Software Radio Attacks & Zero-Power Defenses. IEEE *Symposium on Security & Privacy*, 5/08.