1. Privacy Threats Introduced by Dedicated Short-Range Communications

Abstract—Vehicular Ad Hoc Networks (VANETs) are the pinnacle of 21st Century technology. While vehicular communication via this network offers a variety of positive services, it may be susceptible to malicious attacks and threats. Due to the complexity of this system, it is a high target for cyber terrorism and hacking. To better understand these attacks, we will present threats posed to VANETs. These threats will include vehicle tracking, manipulation of GPS coordinates, impersonation of law enforcement safety devices, and petty crime such as robbery or theft. In addition, we will discuss research and statistics pertaining to General Motors OnStar and the Federal Bureau of Investigation’s (FBI) Stingray Phone Interceptor. These two systems have helped with the development of possible VANET threats because both systems have been manipulated by various personnel resulting in the intrusion of privacy. By exploring OnStar and the Stingray, a clearer roadmap of the possibilities of attacks will be presented. We will conclude by summarizing possible defense methods that OnStar and the Stingray provide for VANETs.

Participants: Lars Kivari and Mathias Masasabi

2. Papers, status of papers, products

Our paper is currently in the draft stage. We have been working to put literature review into the paper along with background information. Our literature review will serve as stepping stones for our advisor George for his research which goes more into depth in the VANET technology.

3. Findings

Because our project (Mathias and mine), was based mostly around literature review, we studied the past research and articles that relates to VANETs and privacy. By pulling McDonald and Cranor’s table in “How Technology Drives Vehicular Privacy”, we were able to add our own rows and columns which include different threats that VANETs may pose.

4. Contributions:

a. One of our contributions include the table extension that we’ve created. We were able to add more threats that VANETs might introduce when they’re implemented. We have also done a literature review that discusses VANETs and previous security threats that they may cause when introduced.

b. to other disciplines: This research and literature review will be helpful for other disciplines because it will be applicable to the criminal justice field and security threats. The computer science and law sectors will be able to work together to come up with solutions to stop the attacks.

d. Beyond science and engineering: This research contributes beyond science and engineering because everyone that drives a car connected to the VANET system in the future will be subject to different privacy threats and attacks. Making people aware of what can happen helps prepare for it.