1 Princples of Cybersecurity

1.1 Fundamentals of Automotive Security

We now step into the realms of cybersecurity in a more detailed manner. Automotive security is a relatively nascent field whose academic origins can be traced back to early days of the ESCAR (https://www.escar.info/history/escar-europe/escar-europe-2003-lectures-and-
html) security conference. The thoeries proposed by the early academics were soon realized and the first car hack papers were published back to back in the years 2010 (Koscher, Karl, et al. "Experimental security analysis of a modern automobile." 2010 IEEE Symposium on Security and Privacy. IEEE, 2010.) and 2011 (Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." USENIX Security Symposium. Vol. 4. 2011.). The first of these papers demonstrated that a attacker with physical access to a vehicle can easily observe and manipulate the vehicles states while the second demonstrated more than technique via which a remote attacker to gain physical access. While these revelations were shocking, a wider and stronger impact was made by three BlackHat/DEFCON presentations (https://www.youtube.com/watch?v=MAcHkASmXEc, https://www.youtube.com/watch?v=OobLb1McxnI, https://www.youtube.com/watch?v=n70hIu9lcYo) and the corresponding Wired article (https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/). Anybody wondoer why Greenday sells more than The Clash in today's internet era? Moving on, this section will use the content of the above mentioned papers/presentations to lay a foundation for the upcoming chapters and creating an understanding for the general principles of cybersecurity.

1.2 Introduction to Cryptography

1.3 Message Authentication

1.4 Encryption on CAN