

[BUSINESS INFORMATION SYSTEM SECURITY]

uNIVERSITY OF PORTSMOUTH |

[tHE risks of COmputer car (INTERNET OF THINGS)]

Panipak Phueabunmak

[2017]

**Abstract**

The Internet of Things (IoT)[[1]](#footnote-1) is the next step in the evolution of wireless network, big data and connected devise. As every sensors shrink in size and transfer from smartphones to other everyday objects. For instance, IPhone recently released an internet connected into App Store (Viper SmartStart) to unlock the car. Computer cars are part of (IoT) now. Moreover, attackers always find vulnerabilities in the car. As the result, once the attacker finds them it can be used to hijack all the car controls. Also they will be able to apply the accelerator, steering, breaks and unlock the doors. The security research by Miller, Valasek (July, 2016) showed a demo on how the “Jeep have been kill on the highway and Jeep vendor recalled 1.4M vehicles for security fix”. In the case, what if the attackers find all the vulnerabilities and use it for dangerous purpose like killing everyone by crashing their cars or damaging all the properties (Golson, 2016). I have chosen to investigate car (Jeep) IoT security with regards to remote control devices and how effective these are at preventing carjackers, information regarding security measures can and will be sourced from manufacturers of network system and (IoT) equipment. Control systems will be studied as the main point of entry for a ‘robus and secure’ against wireless attacker.

**Word count 219**

1. Internet of Things (IoT) is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. In my opinion “If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security” [↑](#footnote-ref-1)