International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1	**VOL**	02
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016	**Accepted**	10 - March – 2016
Article ID	ICSSCCET126	**eAID**	ICSSCCET.2016.126

Review of Keen Remote Gadgets in Vehicle

S Anbarasu[1], P M Mohammed Ashfaq[2], V Ganesh Balaji[3], M Mohanraj[4], K Mohammed Fazil[5]
[1]Assistant Professor Department of ECE, [2,3,4,5] Karpagam Institute of Technology

Abstract—*Modern auto mobiles upgraded with remote innovations, for example, Bluetooth can essentially be considered as remote communicators. Clients can use the upsides of such gadgets by associating them to their savvy mobiles. For instance client can hear sound tones or approaching call tones by means of such remote gadgets. Be that as it may, these sort of remote gadgets works under specific limitations such as security issues, matching with advanced mobile phones. On the off chance that these gadgets are set to the vehicle-arrange, a brilliant programmer in control of such a gadget could execute assaults by infusing subjective messages into the in-vehicle system. These assaults might be rises issues on human life further more influence the wellbeing of vehicles. Subsequently, mind on security ought to be taken while actualizing these gadgets.*

I. INTRODUCTION

Present day vehicles are furnished with various ECUs (electronic control units) in charge of the principle elements of the vehicle. These capacities incorporate the motor framework, slowing mechanism, headlights, power windows, air packs, aeration and cooling systems and so on. In addition, vehicles are getting extra capacities to interact with their environment. There are numerous sensors, for example, cameras, lidars and radars that give information to components, for example, versatile voyage control, path keep help frameworks, crash evasion frameworks and additionally programmed stopping. Furthermore, vehicles are progressively using so as to be associated with the computerized world telematics, Wi-Fi and Bluetooth advancements. These vehicles don't just associate with their surroundings additionally with their clients' gadgets. Thusly, vehicles are currently versatile IoT (Internet of Things) gadgets that are associated with their clients' gadgets. Usefulness, for example, interfacing an advanced mobile phone to the auto's infotainment framework and utilizing the auto's speakers and small scale telephones to make calls is a typical use case. Another normal use case that is turning out to be progressively well known is interfacing an advanced mobile phone to the auto by means of the OBD-2 (On-Board Diagnostics) port and utilizing an application to peruse out different diagnostics information from the auto, for example, motor rate, wheel pace and coolant temperature. A few applications would likewise permit perusing and clearing DTCs (analytic inconvenience codes). This sort of data permits a vehicle client to better comprehend the vehicle condition and help with investigating vehicle in convenience Based on these two above use cases, the focus of this paper is on two types of vehicle IoT devices that could be found in a car: Infotainment systems and OBD-2 port dongles.

In the rest of the paper when we write vehicle IoT devices we mean the above two device types. This paper focuses on one wireless protocol, namely Bluetooth, which is used for connecting user devices to a car. The reasons are as follows. Older versions of Bluetooth have some inherent limitations in the protocol and many Bluetooth-enabled devices in the past have had errors in the implementations [1]. A typical pairing procedure is simple (often using short 4-digit PINs). Moreover, some Bluetooth devices have limited physical input/output capabilities leading to non-configurable settings, especially for the PIN and enabling/disabling the discoverable mode. Last, Bluetooth is extremely common on modern vehicles [2] and in order to provide high usability the configuration options are typically non-changeable or hidden in menus (meaning that the default values are used).

Researchers [3] have shown that if an attacker can exploit the Bluetooth stack implemented in software on vehicle systems, the attacker

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.

could gain access to the in-vehicle network and inject commands such as unlocking the doors, disabling the brakes or killing the engine. It has also been shown that it is possible to brute force a randomized PIN with no user interaction in about 10 hours on average for a specific infotainment system. One can also consider that various data (such as GPS coordinates, VIN or other sensitive data) can be extracted from the vehicle over the Bluetooth communication channel.

Combining the high damage potential of attacks on vehicles with the potential limitations of Bluetooth pairing, vehicle IoT devices are highly desirable targets for attackers. This paper focuses on errors in implementations where Bluetooth security features are not fully utilized. We define errors as something that can be remedied by developers by modifying the implementations to provide the necessary security measures. Examples of errors include not providing user's options to change the default PIN or not allowing users to disable discoverable mode. These limitations could allow attackers easy access to the in-vehicle network via the vehicle IoT device where they could potentially cause major damage to the vehicle and injury to the driver and passengers.

II. Literature Review

This section provides some background on the Bluetooth protocol, some details on the type of devices that we are considering in our survey and a definition of the attacker.

Two Blue tooth-enabled devices typically have to go through a few steps in order to allow the devices to communicate with each other [4], [5], [6]. The devices first establish radio coordination by synchronizing on the same frequency-hopping pattern. If it is the first time the two devices communicate, the devices go through a pairing procedure. For devices supporting up to Blue tooth v2.0 [4], the devices use a PIN (often 4 digits long) to perform pairing. Either one device has a fixed PIN or the user selects a PIN and then the user inputs the same PIN on the other device, or one device generates a random PIN, displays it to the user and the user inputs the same PIN on the other device.

From Blue tooth v2.1 [5], the pairing procedure has been significantly improved by the introduction of Secure Simple Pairing (SSP).It supports four different association modes whereof one is called Numeric Comparison. This mode is suitable for cases where both involved devices have output capabilities in terms of a display. Numeric Comparison displays a 6-digit numeric code on each device. The user then compares the two numbers to ensure that they are identical, and if they are the user confirms the pairing on the device(s) that can accept an input.

To allow a device to go through the pairing process, a device can typically be set to discoverable mode (to consider different gadgets to find it in the event that they hunt down close-by gadgets) and pair able mode (to allow the device to accept pairing requests).

To increase usability and avoid multiple menu choices for users, generally many implementations include the enabling of pair able mode in the discoverable mode setting. That is, the settings menu for a device would often only allow the user to enable or disable discoverable mode (which at the same time also enables or disables pair able mode). The result is that while the device is in discoverable mode and can be found during searches by nearby devices, the device in question would also most likely accept pairing requests. In the rest of paper when we write discoverable mode we also include pair able mode. Thus, as an assumption we define a device that is discoverable as also pair able.

Based on the implementation a device could be always in discoverable mode or a user is required to enable discoverable mode by pressing a button or selecting such an option in a menu.

Bluetooth devices support a number of Bluetooth profiles [7]. The profiles indicate which benefits a gadget bolsters. The profiles can be seen as "modules" that are on top of the Bluetooth Core specification to give extra components and capacities. Below, we give a few examples of profiles that typically are supported by vehicle IoT devices.

- **SPP** - Serial Port Profile. This profile defines the protocols and procedures to be used by devices using Bluetooth for RS-232 serial cable emulation. It is used by for example OBD-2 dongles.
- **HFP** - Hands-Free Profile. This profile is used to allow the infotainment system to communicate with mobile phones in the car. The infotainment system could access some of the phone's features remotely to for example make calls.
- **PBAP** - Phone Book Access Profile. Using this profile, Phone Book Objects could be shared between the info- tainment system and a mobile phone to display the name of the incoming caller on the infotainment system or to download the telephone directory so the client can start a call from the showcase on the infotainment framework.

As mentioned in the previous section, the focus of this paper is on two types of Bluetooth devices that could be found in a car:

1) Infotainment systems

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.

2) OBD-2 port dongles

For infotainment systems, we break down the categorization further into:

a. Built-in infotainment systems
b. External infotainment systems

Built-in infotainment systems are the systems that come preloaded in the car when the car is purchased. They are typically connected to the in-vehicle network to provide the user with various additional functionality such as controlling the air conditioner or displaying a video feed from the parking assist camera. Infotainment systems in general provide decent physical input/output capabilities in terms of buttons, knobs, touch screen and displays. If the built-in infotainment system is exploited, an aggressor could possibly infuse CAN (Controller Area Network) messages into the in-vehicle system to execute discretionary capacities on the ECUs [3]. The exploit may require a secondary step to break out of the Bluetooth application running on the infotainment system since access only to the Bluetooth application would allow the attacker only to access the services provided by the Bluetooth application, e.g., as mentioned above HFP, PBAP etc. However, if the attacker is able to exploit the Bluetooth application and gain control of the infotainment system, the attacker could potentially send CAN messages on the in-vehicle network to perform arbitrary actions [3], [8], [9], [10].

External infotainment systems are commonly just connecting speakers and microphones to the vehicle and would not have any connection to the in-vehicle network. As a result, if the external infotainment system is exploited, an attacker would be limited to only accessing the infotainment system itself (i.e., accessing the above mentioned Bluetooth services to for example read out contact entries from the address book) but not be able to access the rest of the ECUs in the in- vehicle network. Similar to built-in infotainment systems, external infotainment systems typically provide decent physical input/output capabilities.

OBD-2 port dongles are small palm-sized devices that plugs into the OBD-2 port on vehicles. By and large, these dongles need complex physical information/yield capacities, i.e., there is no keypad on the gadgets to permit any data and no showcase to permit any yield. These dongles are associated with the OBD-2 port and have direct access to the in-vehicle system. Clients can utilize an application on their advanced cell and interface with the dongle over Bluetooth to see different diagnostics information extricated from the vehicle, for example, motor RPM, vehicle speed, coolant temperature, GPS organizes and so on. On the off chance that the dongle is misused, an assailant could infuse CAN messages specifically into the in-vehicle system to execute subjective capacities on the ECUs.

Among the three vehicle IoT gadgets we are investigating, the OBD-2 port dongle is the most unsafe gadget as it gives a direct entry point to the in-vehicle system to send CAN messages. Specialists have demonstrated that if an assailant can infuse self-assertive CAN messages into the in-vehicle system, it is conceivable to execute various distinctive assaults, for example, killing the lights, sounding the horn, murdering the motor, debilitating or bolting the brakes, yanking the guiding wheel and so on [8], [9]. These sorts of assaults could have genuine results on the security of drivers and travelers.

A brief definition of the attacker is as follows: The attacker uses her own Bluetooth device to connect to the vehicle IoT device (infotainment or OBD-2 port dongle). The goals of the attacker are:

- Pair own device to vehicle IoT device by knowing or guessing the fixed PIN
- In case of OBD-2 port dongle: Inject CAN messages into in-vehicle network to perform arbitrary actions (such as unlock doors, trigger the air bags, lock the brakes etc.) [8], [9].
- In case of infotainment system: Exploit Bluetooth soft- ware on infotainment to gain access to the in-vehicle network or extract private information about user from the infotainment system (phonebook and calendar entries, and other potentially sensitive data) [3].

III. Survey Results

This section provides the survey results of the vehicle IoT devices. As described in previous sections, an attacker that is able to connect to a vehicle IoT device and if necessary exploit the system to be able to send CAN messages on the in-vehicle network could execute a number of serious attacks. To understand how easy or difficult it would be for an attacker to connect to a vehicle IoT device, we conducted a survey on vehicle IoT devices (Bluetooth interfaces on infotainment systems and OBD-2 port dongles).

The purpose of the survey is to understand what kind of security vehicle IoT devices offer and to what degree the user is able to enforce security. Based on the results of the survey, we discuss errors in implementations and provide some suggestions on improvements for security.

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.

The survey was conducted as follows. We investigated large number (over 100) vehicle IoT devices comprising both built-in and external infotainment systems as well as OBD-

2 port dongles. For each device we investigated whether the device uses a fixed or dynamic PIN. Additionally, we investigated whether the connecting device (e.g., smart phone) initiates the pairing by searching for the vehicle IoT device in discoverable mode or if the vehicle IoT device is searching for the connecting device in discoverable mode. We also determined whether a user is required to perform any steps to put the vehicle IoT device into discoverable mode or if the device is always in discoverable mode.

As we do not disclose the actual manufacturers, models or device names, we unfortunately cannot provide a concrete list of references for the investigated devices. However, all information used in the survey is public information found on the Internet, typically found in product user manuals. It should be noted that the survey and the corresponding analysis are purely based on documentation materials and that there were no actual practical testing conducted.

An overview of the survey results are shown in Table I. The IoT device column shows the categorization of Built-in infotainment, External infotainment and OBD-2 port dongle.

Next segment PIN fixed/dynamic shows whether the PIN is fixed or element. Settled client configurable implies that the client can change the PIN to fixed esteem yet unless it is transformed it will have a default esteem. Settled unchangeable implies that the PIN is fixed to specific esteem at generation and can't be changed by the client. Dynamic implies that amid the matching methodology the client chooses a PIN freely or a PIN is created by the gadget. SSP: Numeric correlation implies that no PIN is inputted on the gadgets yet rather the client assesses the 6-digit code on both gadgets and acknowledges on the off chance that they coordinate.

The PIN section portrays on account of fixed PIN the real unchangeable or default PIN, and if there should be an occurrence of element PIN User information or arbitrary implying that the client chooses a PIN voluntarily and inputs into the two gadgets or that the PIN is haphazardly created on the vehicle IoT gadget and the client peruses the PIN off the presentation and inputs into the interfacing gadget. If there should arise an occurrence of SSP N/A shows that no PIN is utilized.

The following section Discoverable mode clarifies the find capable method of the vehicle IoT gadget. Continuously enabled1 implies that the client has no real way to cripple the discoverable mode (which would leave the gadget helpless to aggressors attempting to combine with it) the length of Bluetooth is empowered. Client needs to empower implies that the vehicle IoT gadget is normally in non-discoverable mode and just when the client needs to combine a gadget the client needs to empower discoverable mode. N/A auto scans for associating gadget implies that the vehicle IoT gadget is for all time in non-discoverable mode. The associating gadget should be put into discoverable mode and the vehicle IoT gadget scans for the interfacing gadget.

The last segment No. of gadgets records what number of the overviewed gadgets fit into particular class.

Typically, while the Bluetooth usefulness is empowered, the vehicle IoT gadget is in discoverable mode; notwithstanding, in a few cases there appears to exist a capacity that would compel the gadget to go into non-discoverable mode after a specific measure of slipped by time (e.g., 2 minutes). This clock capacity is however not portrayed in any documentation we discovered so we accept that any gadget that is classified as always empowered is dependably in discoverable mode.

IV. Analytical Report

This section presents a discussion and an analysis on the results in previous section. We also provide some suggestions for improving the security. We discuss and analyze each vehicle IoT device type (built-in infotainment systems, external infotainment systems and OBD-2 port dongles) separately.

A. Built-In Infotainment Systems

There are five classifications for this sort. Altogether we studied 44gadgets. Out of these, 13 gadgets appear to never be in discoverable mode since the vehicle IoT gadget scans for the interfacing gadget. This methodology requires the client to effectively utilize the vehicle IoT gadget to scan for and pair with the associating gadget. 11 out of these 13 gadgets use dynamic PINs, i.e., either the client picks a PIN amid the matching system or an arbitrary PIN is produced and showed on the vehicle IoT gadget's showcase and the client inputs the same PIN on the interfacing gadget. The eleventh gadget utilizes a fixed client configurable PIN, which is set to 1111 as a matter of course yet can be changed. For the remaining 31 gadgets, the client needs to empower discoverable mode on the vehicle IoT gadget ordinarily by selecting a choice in the menu. Out of these 31 gadgets, 18 gadgets use dynamic PINs and 13 gadgets use fixed client configurable PINs where the default PINs are 0000, 1234, 1111 and 1212. The last 2 Gadgets use fixed unchangeable PINs (1234).

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.

In view of the overview comes about the client needs to either empower discoverable mode or the vehicle IoT gadget is never in discoverable mode. This methodology keeps an aggressor from effectively finding the vehicle IoT gadget and attempting to match with it. In addition, 29 gadgets use dynamic PINs which make it substantially more difficult for an aggressor to attempt to combine with the vehicle IoT gadget. The main recommendations we make for this sort is that However, the vehicle IoT gadget might in any case be in pair able mode regardless of the fact that it is in non-discoverable mode and it would be workable for an assailant to scan for the vehicle IoT gadget utilizing its Bluetooth deliver and attempt to combine with it [1], [3].

B. External Infotainment Systems

For outer infotainment frameworks, 60 gadgets were surveyed and classified into eight classifications. 20 gadgets support SSP: Numeric examination which gives an enhanced blending methodology. Out of these 20 gadgets, 5 gadgets appears to never be in discoverable mode as the auto scans for the associating gadget, 3 gadget requires the client to specifically empower discoverable mode and 12 gadgets appear to be dependably be in discoverable mode when Bluetooth is empowered. In any case, subsequent to SSP is utilized; client cooperation is required on the vehicle IoT gadget to acknowledge the matching demand in any case. 33 gadgets use fixed client configurable PINs where the default PIN is 0000. Out of these, 6 gadgets are never in discoverable mode as the auto needs to hunt down the interfacing gadget and 8 gadgets require the client to empower discoverable mode. The remaining 19 gadgets appear to be dependably in discoverable mode. At last, 7 gadgets use fixed unchangeable PINs (0000 and 1234). 4 of these require the client to empower discoverable mode while 3 gadgets are dependably in discoverable mode.

An aggressor might have the capacity to interface with the gadgets that are dependably in discoverable mode with fixed unchangeable PINs and fixed client configurable PINs if the default PIN has not been modified. In light of our overview, around 41% (19 out of 46) of the gadgets researched are helpless. Be that as it may, following the outer infotainment framework is not associated with the in-vehicle arrange, the potential harm an assailant can bring about is restricted. Proposed efforts to establish safety are again to keep away from fixed client configurable and fixed unchangeable PINs and in addition to utilize non-discoverable mode as default and permit the client to empower it when vital or permit the client to handicap discoverable mode. Since infotainment systems typically offer decent physical input/output capabilities it is recommended to use dynamic PINs or include a menu option to enable/disable discoverable mode. Moreover, SSP: Numeric comparison should also be used if the connecting devices support it.

C. OBD-2 port dongles 35 OBD-2 port dongles were surveyed and categorized into four categories. 5 devices use SSP: Numeric comparison whereof 3 devices require the user to enable discoverable mode on the IoT device and 2device is always in discoverable mode. One thing to note is that even though SSP: Numeric comparison is used, the dongles that we surveyed lack sophisticated output capabilities (i.e., display) to actually show the value to be compared to the user. In other words, the user has to blindly accept the 6-digit value displayed on the connecting device without comparing that value to the one that is supposed to be shown on the dongle. Basically, the numeric comparison association model is not meant for this use case and it offers no better protection than the Just Works3 model. The remaining 30 devices use fixed PINs and are always in discoverable mode when Bluetooth is enabled. 2 of these devices uses a user-configurable PIN with a default value set to the serial number of the device. That is, each of these devices is initially configured to use its own unique PIN as default value (assuming that serial numbers are unique). Once the initial pairing has been completed, the user changes the PIN to something else. The final 28 devices use fixed unchangeable PINs with values such as 1111, 1000 and 4567.

An attacker may be able to connect to the devices that are always in discoverable mode using fixed unchangeable PINs or SSP: Numeric comparison. From the results of our survey 89% (25 out of 28) of the investigated devices are susceptible. For the fixed unchangeable PIN devices, an attacker can guess the PIN based on the typical values used (1111, 1000 and 4567) to pair with the vehicle IoT device. For the device supporting the SSP approach where the device is always in discoverable mode, an attacker only needs to send a pairing request since no actual comparison is required (no output capabilities on the OBD-2 port dongle and no input capability to accept the pairing request). If an attacker is able to successfully pair with an OBD-2 port dongle, an attacker could execute a wide range of attacks by sending arbitrary commands to the in-vehicle network. Since the OBD-2 port dongle offers direct entry into the in-vehicle network it is imperative that this entry point supports proper security measures. The reason for the large number of devices with fixed unchangeable PINs is mainly because the dongles have limited physical input/output capabilities, i.e., no keypad to input a PIN and no screen to display any randomized PIN. The 3 Just works is a Secure Simple Pairing association model introduced with Bluetooth v2.1. Basically, Just Works follows the same pairing procedure flow as Numeric Comparison except that the user does not verify any 6-digit numbers at the end of the pairing process. Therefore, this method offers no man-in-the-middle protection [5]. Dongles might just have a physical catch as information and a couple of LEDs as yield. Accordingly, contemplating above, we propose the accompanying efforts to establish safety. Clients ought to have the capacity to empower discoverable mode by for instance squeezing a physical catch on the gadget and there ought to exist an approach to handicap discoverable mode either by pushing a catch or utilizing a clock capacity to incapacitate discoverable mode after a specific measure of time (e.g., 1 minute). In the event that fixed PINs are unavoidable, client configurable PINs utilizing one of a kind and long (e.g., 16 digits) default PINs are favored where the client is prescribed to change the PIN after the introductory matching. In the event that fixed unchangeable PINs are

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.

unavoidable, gadgets ought to be preloaded with extraordinary (to the degree conceivable) and long PINs taking into account for instance the gadgets' serial number to stay away from worldwide PINs.

V. Conclusion

As the outcomes and investigation of the review appear, there are a few distinctive methodologies for matching client gadgets (e.g., advanced mobile phones) with vehicle IoT gadgets (infotainment frameworks and OBD-2 port dongles) over Bluetooth. The outcomes show that it is most difficult for an assailant to combine with implicit infotainment frameworks as they require client cooperation to permit a remote gadget to be matched. For outer infotainment frameworks about 40% of the overviewed gadgets could permit an aggressor to combine with the gadget by speculating a fixed PIN. At long last, for OBD-2 port dongles, near 90% of the explored gadgets could permit an aggressor to match with the gadget by sending so as to speculate a fixed PIN or just a blending demand. In the event that an assailant effectively figures out how to combine with an OBD-2 port dongle, an aggressor could perform various assaults by injecting messages specifically into in-vehicle system. We give recommendations including maintaining a strategic distance from fixed PINs and requiring client collaboration to empower discoverable mode. Cutting edge vehicles are versatile IoT gadgets supporting different remote conventions, for example, Bluetooth. Utilizing Bluetooth as an entry point, assailants could target vehicles to execute assaults conceivably prompting real harm to the vehicles and wounds to drivers and travelers, in this way accentuating the requirement for appropriate efforts to establish safety.

References

1. Dennis K. Nilsson, Phillip A. Porras and Erland Johnson, How to Secure Bluetooth-based Pico Networks, SAFECOMP, 2007
2. Charlie Miller and Chris Valasek, A Survey of Remote Automotive Attack Surfaces, DEFCON 22, 2014.
3. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Conference on Security, 2011.
4. Bluetooth SIG, Bluetooth Core Specification Version 2.0 + EDR, 2004.
5. Bluetooth SIG, Bluetooth Core Specification Version 2.1 + EDR, 2007.
6. Bluetooth SIG, Bluetooth Core Specification Version 4.1, 2013.
7. Bluetooth SIG, Bluetooth Specifications and Bluetooth Profiles, https://www.bluetooth.org/en-us/specification/adopted-specifications
8. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy, 2010.
9. Charlie Miller and Chris Valasek, Adventures in Automotive Networks and Control Units, DEFCON 21, 2013.
10. Dennis K. Nilsson and Ulf E. Larson, Simulated Attacks on CAN Buses: Vehicle virus, ASIACSN, 2008.

Cite this article as: S Anbarasu, P M Mohammed Ashfaq, V Ganesh Balaji, M Mohanraj, K Mohammed Fazil. "Review of Keen Remote Gadgets in Vehicle". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 625-630. Print.