EDITORIAL PREFACE

Vehicular Security*:*
Hackers Moving to the Roads in a Bid to Increase Attack Surface

Kevin Curran, School of Computing and Intelligent Systems, University of Ulster, Londonderry, UK

In recent years, vehicles have evolved to contain a complex network of numerous independent computers and electronic control units (ECUs). ECUs perform a variety of functions such as measuring the oxygen present in exhaust fumes and adjusting the fuel/oxygen mixture improving efficiency and reducing pollutants. Over time these ECUs have become integrated into nearly every aspect of a vehicle's functioning, including steering, cruise control, air bag deployment and braking. Some modern cars such as the Mercedes-Benz contain over 20 million lines of code and possess nearly as many ECUs as an Airbus A380. It is expected that vehicles will soon contain 300 million+ lines of software code. This demonstrates the vulnerable nature of next generation vehicles. In addition, not only do these ECUs connect to each another but they now can connect to the Internet, making vehicle computers as vulnerable to the same digital dangers widely known among other networked devices such as trojans, viruses, denial-of-service attacks and more. It is common for new vehicles to have numerous connectivity modes such as Bluetooth connectivity, short-range wireless access for key fobs and tyre pressure sensor not to mention support for satellite radio and inputs for DVDs, CDs, iPads and USB devices.

As electronics and related code become more integrated into modern vehicles, we are reaching a point where they will require similar protection as smartphone, tablets and traditional computers. There is a real worry about hackers controlling vehicles in different scenarios such as having fun with the songs being played, downloading rogue apps, disabling the vehicles ignition, to overriding braking systems. This is a reminder of the early Internet, as Security has not received a great deal of attention from car manufacturers yet. To date we have not seen any widespread reporting of the issue but those conducting work in this area will tell you that these are probable attacks. Controlled experiments have shown that vehicles can be controlled via the telematics systems and some have successfully embedded malware into the music centre over wireless connections. The Center for Automotive Embedded Systems Security in Washington team demonstrated how

to bring a wide range of systems under external control, such as the engine, brakes, locks, instrument panel, radio and its display. The attackers posted messages, initiated annoying sounds and even left the driver powerless to control radio volume. They also attacked the Instrument Panel Cluster/Driver Information Center displaying cheeky messages and altered the fuel gauge and speedometer readings, adjusted panel illumination. Subsequent hacks took over the Engine Control Module which lead to uncontrollable engine revving, readout errors and complete disabling of the engine.

All modern vehicles possess 'On-Board Diagnostics' port which allow mechanics to diagnose faults and retrieve information on the vehicle's performance and in some cases change aspects such as the timing of the engine. The almost universal controller area network bus on vehicles - known as the CAN bus makes such breaches possible. This is becoming the main access point for hackers as everything can be changed using this port. We can breathe a little sign of relief at present as important aspects such as the speed control, steering and brakes are all located on a separate vehicle network, there is still interconnectivity between both vehicle network backbones so that a breach in one can cause havoc in the other. It is presently still a difficult system to breach but as more and more exploits get shared on the Internet, there is much cause for worry. The vehicle mobile phone hardware providing a connection to the on-board computer system is also vulnerable to malware being installed which could allow a thief to unlock the car remotely and steal it. This is serious as is already talks of an app store for vehicle apps.

Vehicle 'operating system' security currently resides with the manufacturers (i.e. you cannot install McAfee anti-virus) but it is advisable to familiarise oneself with aspects such as the remote shutdown feature. For instance, who and what can cause that system to shut the car down. Also, one should be careful when installing third-party electronic accessories as they may not be as rigorously designed as an original manufacturer feature. If you are extra paranoid, you may want to restrict access to the OBD-II diagnostic port. This is a key diagnostic port used by service mechanics but it is also a key attack vector to upload malicious code.

The motivation to build rigorous and secure systems should be there because it is quite possible that all involved in its design could be held liable if a defect caused or contributed to a collision. A saving grace for now is there are not many motivations to stealing vehicles via a sophisticated hack because of the complexity involved and sophisticated tools needed. It is still easier to use a Slim Jim. However that might change in the days ahead and vehicle manufacturers and telematics installers need to concentrate on all the vulnerable entry points and insert firewalls to restrict access to integrated systems such as the radio and music system and on-board diagnostics port. They urgently need to update the security of automotive computer systems starting today.

So on to this issue of IJACI. Wanga, Liua, Xiea and Zuoa in "Weight-aware Multidimensional Advertising for TV Programs" declare that given ongoing developments in the digital television industry, the consumption habits of consumers are substantially influenced by advertisements, which become the main revenue source for TV broadcasters. Therefore, the effective deployment of advertisements is necessary. Digital television is a thriving sector and the number of channels continues to increase, so that the various dimension information of data on electronic programming guides overwhelm the advertisement recommendation systems for TV programs. In this paper, present a weight-aware multidimensional model approach that focuses on the different weights of advertisement or program content parameters and their interrelationship. This study is actually the first attempt at applying the approach to advertisement recommendation. They introduce an empirical measure for obtaining the weight values of dimensions, and present the similarity measure model, which enhances accuracy and convergence in advertisement recommendations. clustering technique.

In "Integrated Network Topological Control and Key Management for Securing Wireless Sensor Networks" by Kumar and Nagarajan, we see that wireless sensor networks are increasing in popularity due to their low-cost, self-organizing behaviour and sensing ability in diverse environments. One of the most challenging topics in relay network is security. The existing Network topology acquisition processes for non transparent mode relay networks are not effective in providing security features and it is critical to provide privacy and validation in order to prevent information from relay networks. In their proposed system, key management provides privacy along with validation of security on relay nodes. The Security is designed with consideration of the multi cluster based topology control through a multiple intensity keying and has low energy requirements.

Brinka, Alonsob and van Bronswijka in "Assessing smart-home platforms for Ambient Assisted Living" discuss smart-home platforms which support applications, services, and devices for Ambient Assisted Living (AAL). The developers of those platforms commonly focus on technological requirements only, without having a clear understanding of end-users such as older adults living independently. Moreover, since there are no functional testing methods for AAL platforms, they introduce a testing methodology for smart-home platforms and use it to test two platforms for their suitability: the universAAL platform that is based on an ontology model, and the 'Universal Plug and Play' (UPnP) platform in combination with 'Digital Home Compliant' (DHC) framework (first version), both using fixed terminology and descriptions. They first developed a comprehensive overview the support older people may need from a smart home and then they developed scenarios that cover many of those needs and used the scenarios as test cases in functional tests in a simulation environment. The results show that 4/5 of the smart-home applications in the AAL scenarios will not work without a platform extension thus demonstrating the importance of these extensions. Therefore, the use of an ontology model for platforms is advisable because of its quick and easy adaption to new devices and services, needed for the worldwide rollout of smart-homes for AAL.

Finally, in "UWB Indoor Location for Monitoring Dementia Patients – The Challenges and Perception of a Real-Life Deployment" Grünerbl, Bahle, Hanser and Lukowicz outline how monitoring the activities of daily living is a common form of assessing the progression of dementia. Yet so far, this mostly can only be done by visual observations, which is time and cost expensive and therefore only done on a short scale. Even though the technology for automatic monitoring exists, it is still seldom used in real life environments. Key problems are the effort involved in sensor deployment and the extraction of relevant activity information from simple sensor data. Here they describe a long-term real-life monitoring of dementia patients using an easy to deploy UWB-location system along with practical deployment and monitoring results.

Enjoy!

Kevin Curran
Editor-in-Chief
IJACI

Kevin Curran BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr Curran has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 700 published works. He is perhaps most well-known for his work on location positioning within indoor environments, pervasive computing and internet security. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to BBC radio & TV news in the UK and is currently the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Technical Expert for Internet/Security matters. He is listed in the Dictionary of International Biography, Marquis Who's Who in Science and Engineering and by Who's Who in the World. Dr Curran was awarded the Certificate of Excellence for Research in 2004 by Science Publications and was named Irish Digital Media Newcomer of the Year Award in 2006. Dr Curran has performed external panel duties for various Irish Higher Education Institutions. He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computing Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE) and a fellow of the higher education academy (FHEA). Dr. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He is the Editor in Chief of the International Journal of Ambient Computing and Intelligence *and is also a member of numerous Journal Editorial Committees and numerous international conference organising committees. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies.*