Securing CAN Bus Communication: An Analysis of Cryptographic Approaches

Jennifer Ann Bruton

M.Sc. in Software Engineering & Database Technologies

National University of Ireland, Galway

Discipline of Information Technology

College of Engineering & Informatics

August 2014

Head of IT Discipline:

Dr. Michael Madden

Research Supervisor:

Dr. Michael Schukat

Contents

List of Tables

List of Figures

Abstract

The security of the Controller Area Network (CAN) within automotive applications is becoming significantly more important for maintaining a safe and private driving experience but the CAN bus itself has no security features. Recent articles have highlighted the potentially devastating consequences that can arise when this network is successfully compromised. Research into the area of embedded systems security, and automotive security in particular, is a relatively nascent area. Most efforts concerned with improving CAN security using software-based cryptographic methods have focussed on message authentication, where the challenge of dealing with a small packet frame is considerable. The aim of this research is to further investigate the effects of using cryptographic approaches for both encryption and authentication to improve the security of CAN bus communications. This thesis presents an experimental platform based on the BeagleBone Black, SocketCAN and OpenSSL library for testing cryptographic methods on a CAN bus. Different cryptographic schemes concerned with AES and RC4 encryption, HMAC message authentication, and authenticated encryption are designed and deployed on this platform. The experimental results collected as part of this research confirm that the security of the CAN bus can be improved using cryptographic techniques, and that there are consequences with respect to message times as a result of applying these security measures. This research also highlights elements of the CAN bus communications context and aspects of the cryptographic designs that suggest directions for future development.

1 Introduction

1.1 Problem Context

In the modern world, the proliferation of computer systems, together with their networking and interconnection, has created a significant dependence by governments, organizations, and individuals on the data stored, processed, and exchanged using these systems; thus, these computer resources and their data/information are valuable assets that need to be protected. Computer security is concerned with providing the necessary safegaurds for an information system in order to protect the confidentiality, integrity and availability of its resources, data and services; any additional benefits of using computer technology are only realized if these systems are secure from malicious attacks. Providing sufficient computer security can be challenging due to the fact that system resources possess multiple vulnerabilities that allow that system to become compromised in such a way that it delivers an incorrect output, or that its confidentiality is endangered, or it operates so slowly that it has effectively been rendered unavailable.

Security countermeasures are employed to ideally prevent a security attack from taking place, or to minimize and/or record the effect of such an attack if prevention cannot be accomplished. No single countermeasure can succeed in thwarting all attacks, so the principle of 'defence-in-depth' is often advocated and adopted, where a number of layers of security, using different strategies, are employed. Cryptographic strategies involve the conversion of data into a secret form so that some, or all, of authentication, confidentiality, integrity and non-repudiation requirements can be achieved.

An embedded system is an electronic device that contains a combination of one or more microprocessors and software to carry out a very specific function within a larger system. Embedded systems have gained huge popularity in recent years and, due to their interconnectivity, feature heavily within the 'Internet of Things' vision . As a result of this interconnectivity, they offer great attack opportunities (attack surface) to malicious adversaries and, at the same time, pose great challenges for security provision due to their limited resources, low costs, often strict safety requirements, (e.g. in medical applications) and relative newness in the computer security context.

The use of electronics in automobiles to provide better vehicular performance, passenger safety, and enhanced entertainment facilities, involves the networking together of embedded micro-controllers known as electronic control units (ECUs); a standard automobile contains approximately 50-100 of this units. For in-vehicle communications, the Controller Area Network (CAN) is the preferred bus when exchanging data as it is reliable and works well in noisy, electromagnetic environments.

1.2 Thesis Statement

This thesis focuses on the aforementioned CAN bus and the software-based cryptographic measures that could potentially improve its security. The research question to be answers by the thesis is: "what effects will cryptographic approaches have on the security of the CAN bus and whether the consequences for (time) performance that arise from any improvements in security will be acceptable?" The thesis statement is, therefore:

***

An investigation of the use of cryptographic approaches to secure the Controller Area Network (CAN) bus for real-time automotive embedded systems communications, where performance requirements and resource constraints are strictly defined.

***

1.3 Significance of the Study

Security measures to achieve the goals of confidentiality, integrity and availability for automotive embedded systems can be lacking (Koscher et al., 2010) but their provision is becoming increasingly important. Automotive systems security poses a development challenge due to the limited resources in terms of memory, storage, computational power and bus capacity available to embedded devices. The native CAN bus itself has no security and, as the bus operates in broadcast mode, all ECUs or nodes connected to the bus receive the same messages . Historically, up to about a decade ago, the security of the CAN bus was interpreted as its ability to transfer data with appropriate error detection, error signally and self-monitoring; it was deemed unlikely that an attacker could easily access this network.

Unfortunately, this historical view has recently been proven to be incorrect and internal attacks on the in-vehicle network often specifically target the weaknesses of the CAN bus to compromise elements of the CIA security triad. Recent studies have shown that successfully accessing a single node on the network allows the entire vehicular network to be compromised. Havoc has been shown to ensue when the engine, brakes, doors, power steering, instrumentation, electric windows, radio, warning lights, diagnostic unit, driver information console, and air-bags have been accessed by attackers. The ability of a malicious party to compromise these automotive components leads to significant safety, commercial and data privacy concerns. The CAN bus is also gaining popularity in industrial automation environments and the need for safe operation in these settings is also highly important.

The hard real-time requirements for communications to and from the ECUs, and the constraints of the CAN protocol itself, present challenges for improving the security of the CAN bus. This study will investigate software-based cryptographic approaches to address these challenges, and, if successful, will demonstrate improved CAN bus security without incurring unacceptable delays in communications and without the need for additional, costly, hardware resources.

1.4 Thesis Scope

Given the thesis statement above, and the problem domain outlined, this thesis will examine the following areas of embedded systems and CAN bus technology.

- Automotive field bus technology: the physical properties of the CAN bus and the elements of the CAN bus protocol will be examined; some context for the CAN bus will be created by briefly describing alternative vehicular bus technologies.

- Communication protocols: the CAN bus protocol will be used for communications on the CAN bus; other communication protocols may be used for any out-of-band (not using the CAN bus) communications that may be required, e.g. for key distribution.
- Embedded system / real time operating systems: as the nodes connected to the CAN bus are embedded systems that perform in real-time, the communication system will be supported by an operating system, the appropriate characteristics and mechanisms of which will need to be understood and manipulated.
- Open source software for embedded systems: both the embedded operating system and any software to manipulate and measure the CAN bus messages will be open source.
- Cryptographic approaches for improving the security of the CAN bus, in particular, the elements of computer security that will be explored in this thesis are:
  - Encryption - in order to provide message content confidentially, encryption techniques will be employed; due to the hard real-time nature of the CAN bus, the focus for payload encryption will be symmetric encryption.
  - Message authentication - the basic CAN protocol does not have a field to authenticate the sender, therefore message authentication schemes will be investigated.
  - Key distribution - the distribution of keys to only trusted nodes for securing the communications payload will be explored.
  - Testing and measurement methodologies - the design of appropriate tests to confirm or negate the validity of a given cryptographic approach, and the measurement of time- and/or resource-related performance measures will be established.

7 Conclusions

7.1 Introduction

This section of the thesis contains the insights that have been obtained from the test results collected from the experiments conducted in the previous section. It presents conclusions about how these results address the research question "what effects will cryptographic approaches have on the security of the CAN bus and whether the consequences for (time) performance that arise from any improvements in security be acceptable?" presented in the introduction. Limitations of the designs that are exposed by the results are presented, and opportunities for further research and development are outlined.

7.2 Meeting the Success Criteria

There are a number of success criteria for the thesis set out in Section 1.5 and these can be evaluated based on the results and documentation presented in this report.

An extensive literature review is present that highlights the issues surrounding embedded systems security, automotive security and CAN bus security; this review gathers and evaluates the efforts that have already been made to improve the security of CAN bus communications. This review reveals that few published articles include experimental details from a physical CAN bus, and that many schemes focus on one particular aspect of CAN bus security. The cryptographic approaches identified for improving CAN bus security are message authentication and symmetric encryption, although most articles have concentrated on message authentication with symmetric encryption enjoying very limited utilization.

One of the key contributions of this thesis is the implementation of the proposed security designs on an actual CAN bus experimental platform. The low-cost BeagleBone Black with its AM335x microprocessor is shown to be effective at facilitating CAN bus experiments; the number of CAN bus channels available on each BBB can be extended with the use of a dedicated cape. The use of the Linux kernel to support the CAN bus networking system using `SocketCAN` and `can-utils` is a relatively new concept that has been exploited very successfully in this thesis to deliver the experimental framework for testing CAN bus communications. The utilization of the OpenSSL library to provide both symmetric and asymmetric cryptographic approaches as part of the designs for CAN bus security is also demonstrated as effective, although some of the more recent hash functions and lightweight ciphers are not available with this library. The 3 scenarios established for experimental testing allow a thorough investigation of CAN communications, whether they are to and from the same device, to and from devices on the same micro-controller host, or whether they are to and from devices on separate hosts. The challenges presented by a real network are thus exposed in ways that may not be apparent through software simulation and virtual CAN nodes.

The design and development of software to cater for the different experimental treatments identified in the Introduction to answer the research question is documented in Section 5. It can therefore been concluded that experiments have been successfully established to test the CAN bus platform with no security; with two types of symmetric encryption; with message authentication; for out-of-band key distribution; and for a combination of encryption and authentication. Each of these designs allows the collection of data measurements linked to the timing of CAN bus messages from one node to another and the appropriate presentation, analysis and contextualization of this data allows conclusions to be drawn so that the overall research question can be answered, as indicated in the following discussion.

7.3 Answering the Research Question

The different treatments necessary to address the research question are designed and implemented using the established experimental platform and created software in order to produce results that can inform the answer to the research question.

When there are no cryptographic approaches applied, it has been clearly demonstrated in Figure 34 that it is a relatively straightforward task to access the CAN bus using an oscilloscope (or other probe), to capture data from the the CAN bus, and to interpret this data once the CAN frame layout is known and understood. It has also been shown in Section 4.3 on low-level CAN communications, that a single CAN transceiver can be used to transmit signals onto the CAN bus. It can be surmised, therefore, that any successful cryptographic approaches will improve this situation in some way, i.e. if the data is encrypted it will be harder to read, if the message has authentication, it will be harder to inject external messages.

The effects of any cryptographic approach will be different for each CAN network, depending on the underlying hardware capacity of that network. It has been shown in Section 6.1.3 that a number of factors can influence the outcome of the experiments in this thesis, and therefore the most appropriate way to carry out any further experiments, is to use exactly the same test configuration each time. This does mean that quantitative results obtained from an individual treatment are not very useful, but comparing results for different treatments using the same experimental platform, allows conclusions to be drawn. The experiments performed when there are no cryptographic effects in place establish a benchmark for this comparison, although a hard limit of $1ms$ is also defined.

Using symmetric block cipher encryption with a pre-shared key for CAN bus communication is shown to be effective at making the original message payload secret (Figure 55), and the encryption time not very onerous (Figure 57), so it can be concluded that this is an effective way of securing the confidentiality of CAN messages. Unfortunately, when standard CAN frames of 8 bytes are used, a 16-byte block cipher means that two CAN messages are required for each original message, effectively doubling the message time compared to using no cryptographic approach at all. The doubling of the message time for slower CAN controllers means that the overall time may go above $1ms$ which is unacceptable; it is therefore concluded that this block cipher method should not be used for standard CAN frames; it should be noted that if the CAN FD standard with a 64-byte data field is used, this may be an appropriate approach but preferably when message payloads are close to a multiple of 16 bytes.

The adoption of a stream cipher eliminates the problem of additional messages caused when using the block cipher; it is demonstrated that this encryption also effectively hides the original message content (Figure 58) but that it generates the ciphertext on a byte-by-byte basis so that the encrypted payload is exactly the same size as the original. The weaknesses inherent in the RC4 stream cipher are mitigated in some way by the dropping of the first 512 bytes of the keysteam and by adding a changing value (counter) to the encryption key. However, the use of the CAN identifier field for the nonce is not ideal in this scenario (though it might be acceptable when a 29-bit identifier is used) and when the counter resets, a new encryption key should be used. The increase in message trip time is relatively modest (Table 13), therefore it can be concluded that using a stream cipher does improve CAN bus security without a detrimental effect on message times but that additional effort must be employed to manage the uniqueness of the encryption key.

This work has confirmed that message authentication can be achieved on the CAN bus using HMAC (Figure 62); due to the limited length of the standard CAN data field, the HMAC needs to be truncated and a value of 32 bits was chosen for this. The effect of appending the HMAC to the message limits the message to 4 bytes, and messages longer than this will need to be sent over two frames; again, this is not likely to be an issue with CAN FD 64-byte data frames. The additional time required for messages using HMAC is approximately 40% which is a noticeable increase, but still leaves the time lower than the hard $1ms$ limit. If multiple frames are required, then this limit will be breached but this is a natural consequence of appending the macTag to a message. It can be concluded, therefore, that a HMAC approach will improve message authentication but for some messages within a limited frame size, the additional time overhead may be undesirable.

The cryptographic schemes presented in this thesis rely on the robustness of their secret keys, and these keys need to be refreshed in order to ensure that their reuse does not expose vulnerabilities to attackers. New CAN protocols have been previously been established by other authors to distribute keys via the CAN bus but these mechanisms have costs associated with them in terms of messages forgone in order to send the keys, they are not standard and they must be implemented outside of the CAN controller which deals with the regular CAN protocol. Distributing keys out-of-band could leverage existing secure network protocols such as SSL/TLS without impacting the messages on the CAN bus itself. This thesis does demonstrate that this is possible for a considerable time overhead (compared to the CAN bus message times) but has not been integrated with the cryptographic approaches at this point. A conclusion that can be drawn, however, is that cryptographic approaches can improve CAN bus security if an effective key distribution is in place and that the time overhead associated with an out-of-band mechanism suggests that the keys should be requested in advance of when they are actually going to be needed.

One of the main contributions of this thesis is the production of experimental results for a cryptographic scheme that involves both message authentication with timestamping and symmetric encryption. The results obtained clearly show that CAN bus security is improved, and that message times are considerably increased ($\approx 60 - 70\%$) but still lie well below the $1ms$ threshold. However, there are numerous negative consequences for the particular scheme that has been implemented: the counter for the encryption key nonce is limited to 2 bytes, requiring that the encryption key is changed at least every 2^{16} messages; the HMAC tag is only 2 bytes long which in not recommended by NIST and would require that the authentication key is renewed every $2.56s$; the message payload is limited to 4 bytes which would require additional frames for longer message content; the timestamp is highly dependent on synchronous time over the network is suspected to be adversely affected by CAN controller buffering. This last point highlights the benefits of using an experimental platform for the testing as the proposed timestamp feature works extremely well when all the nodes are on the same host but when they exist on different hosts, the timestamp is rendered ineffective as a method for adding uniqueness to the authentication scheme. It is possible that this effect could be missed when simulating a network or when using only a single, multi-channel host.

It is considered that the research question has been answered over a series of different experiments and that the outcomes of these experiments can help to inform future research and work.

7.4 Future Areas for Research & Development

One of the main constraints with the CAN bus communications for this thesis was the lack of availability of CAN FD Controllers on the BBB cape. The investigation of cryptographic methods for the very limited size standard CAN frame is interesting, but the effects and consequences of these cryptographic approaches for the larger payload could also be evaluated.

The overall design for authenticated encryption assumes that all messages need to be authenticated and encrypted; it is likely in a real-world scenario that this might not be the case and the overhead associated with the applying the cryptographic approach could and should be reserved for those messages that require it. Two bits from the CAN identifier field could be reserved, without significant consequence for arbitration, for toggling the encryption and/or authentication on or off for a message.

The use of a timestamp for the authentication aspect of the cryptographic design is proven to be problematical despite the use of the NTP time synchronization protocol to try to address this issue. The use of a counter for the encryption scheme also has limitations, as the way that it is currently used assumes that it is always increasing; however, a node that does not receive a message with an updated counter value may issue a message of their own with a lower, previously used value. Having both a counter and a macTag in the CAN frame has serious negative consequences for the size of the counter,the macTag, and the data frame; employing just a timestamp instead of a counter would avoid this problem but would introduce those issues revealed when the timestamp is used for authentication. Further investigation is required to determine a reliable method of monotonically and consistently updating a counter/timer over the CAN network.

The effect of the OOB key distribution can be further investigated when the key server is running while the CAN bus is active. The key refresh can be triggered in advance based on a timer/counter (though this is then dependent on a reliable scheme for this) and the server-client relationship must be examined to allow the same keys to be distributed to different nodes in the same trusted group even if they have not requested the keys.

The recent announcement by NIST of a new SHA-3 family of hash functions offers the possibility of a hash function for HMAC that uses intermediate state sizes that could provide lightweight alternatives which would be interesting to explore in the constrained context of the CAN bus. This hash function has also been suggested for an authenticated encryption system that could replace the combined approaches used in this thesis. There are also lightweight stream ciphers such as WG-8 that could experimented with for the CAN bus.

The authentication and encryption schemes have been 'bolted' together for the overall design and use the arguably less secure MAC-then-encrypt approach. There are, however, dedicated modes for authenticated encryption such as Galois Counter Mode (GCM) and Counter Mode with CBC MAC (CCM), amongst others. A future research direction could be the investigation of these modes for CAN bus security, particularly for the CAN FD standard.

It is likely that the CAN protocol will persist as the network of choice in automobiles and some automated environment in the medium term, so continued efforts to investigate and improve the security of this network should be made.

8 References

AB, K. (n.d.). *CAN (controller area network).* Retrieved 14th January 2014, from http://www.kvaser.com/en/about-can.html

Abadeh, M. S., Mohamadi, H., & Habibi, J. (2011). Design and analysis of genetic fuzzy systems for intrusion detection in computer networks. *Expert Systems with Applications*, *38*(6), 7067-7075.

Agosta, G. (2012). *The posix socket api.* Retrieved 10th July 2014, from http://home.deib.polimi.it/agosta/lib/exe/fetch.php?id=teaching%3Apsrete&cache=cache&media=teaching:socket.pdf

Albert, A. (2004). Comparison of event-triggered and time-triggered concepts with regards to distributed control systems. In *Embedded World conference* (p. 235-252).

AM335x. (2014). *Am335x sitara processors, technical reference manual* (Tech. Rep.). Dallas, TX, USA: Texas Instruments. Retrieved 20th June 2014, from http://www.ti.com/lit/ug/spruh73k/spruh73k.pdf

Andrews, M., & Whittaker, J. A. (2004). Computer security. *Security & Privacy, IEEE*, *2*(5), 68-71.

Ångström. (2014). *The angstrom distribution.* Retrieved 17th June 2014, from http://www.angstrom-distribution.org/

Arilou Technologies. (n.d.). *Automotive security* (Tech. Rep.). Tel-Aviv, Israel: Arilou Technologies. Retrieved 16th January 2014, from http://www.ariloutech.com/files/Arilou%20Technologies%20-%20CAN%20bus%20with%20threats.pdf

Arilou Technologies. (2010). Feasible car cyber defense. In *10th embedded security in cars (escar) conference.*

Arora, H. (2011). *C socket programming for linux with a server and client example code.* The Geek Stuff. Retrieved 10th July 2014, from http://www.thegeekstuff.com/2011/12/c-socket-programming/

ARTEMIS-JU. (2011). *The ARTEMIS JU research agenda 2012* (Tech. Rep.). Eidhoven, The Netherlands: ARTEMIS European Technology Platform. Retrieved 2nd January 2014, from http://www.artemis-ju.eu/publication/download/publication/201

Associated Press. (2013). Hackers find weaknesses in car computer systems. *FoxNews.com.* Retrieved 8th January 2014, from http://www.foxnews.com/leisure/2013/09/04/hackers-find-weaknesses-in-car-computer-systems/

AUTOSAR. (n.d.). *Automotive open system architecture.* Retrieved 10th January 2014, from http://www.autosar.org/index.php?p=1&up=0&uup=0&uuup=0

Baker, G. (2008). Schoolboy hacks into city's tram system. *The Telegraph.* Retrieved 9th August 2013, from http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

Bashah, N., Shanmugam, I. B., & Ahmed, A. M. (2005). Hybrid intelligent intrusion detection system. *Proceedings of World Academy of Science, Engineering and Technology*, *6*, 291–294.

BBB Cape. (n.d.). *Beagleboard & BeagleBone Black Capes.* elinux.org. Retrieved 5th April 2014, from http://elinux.org/Beagleboard:BeagleBoneBlack#Hardware_Files

BBB Wiki. (n.d.). *Beagleboard:BeagleBoneBlack.* elinux.org. Retrieved 5th April 2014, from http://elinux.org/Beagleboard:BeagleBoneBlack#Hardware_Files

BBC News. (2010). Hack attacks mounted on car control systems. *BBC News, Technology.* Retrieved 8th January 2014, from http://www.bbc.co.uk/news/10119492

Bellavista, P. (2011). Pervasive computing at scale: Challenges and research directions. In *Sensors, 2011 IEEE* (p. 639-642). doi: 10.1109/ICSENS.2011.6127000

Bellovin, S., & Cheswick, W. (1994). Network firewalls. *Communications Magazine, IEEE*, *32*(9), 50-57. doi: 10.1109/35.312843

Bishop, M. (2004). *Introduction to computer security.* Addison-Wesley Professional.

Black, J. P., Segmuller, W., Cohen, N., Leiba, B., Misra, A., Ebling, M. R., & Stern, E. (n.d.). *Pervasive computing in health care: Smart spaces and enterprise information systems.* Retrieved 1st November 2013, from http://www.research.ibm.com/people/l/leiba/Papers/Pervasive-Computing-in-Health-Care.pdf

Blackmore, J., & Monroe, S. (2013). *Overview of 3.3V CAN (controller area network) transceivers.* (Application Report). Dallas, TX, USA: Texas Instruments. Retrieved 1st July 2014, from http://www.ti.com/lit/an/slla337/slla337.pdf

Bloss, R. (2013). Autonomous unmanned vehicles take over on land, sea and in the air. *Industrial Robot: An International Journal*, *40*(2), 100-105. Retrieved from http://dx.doi.org/10.1108/01439911311297676

Bluetooth SIG. (n.d.). *Bluetooth basics: a look at the basics of Bluetooth technology.* Retrieved 28th October 2013, from http://www.bluetooth.com/Pages/Basics.aspx

Bosworth, S. (2008). *Computer security handbook* (5th ed.). John Wiley & Sons.

Brooks, R., Sander, S., Deng, J., & Taiber, J. (2009). Automobile security concerns. *Vehicular Technology Magazine, IEEE*, *4*(2), 52-64. doi: 10.1109/MVT.2009.932539

Broy, M., Kruger, I., Pretschner, A., & Salzmann, C. (2007). Engineering automotive software. *Proceedings of the IEEE*, *95*(2), 356-373. doi: 10.1109/JPROC.2006.888386

BusyBox. (n.d.). *Busybox: the swiss army knife of embedded linux.* Retrieved 10th July 2014, from http://www.thegeekstuff.com/2011/12/c-socket-programming/

CAN-BUS shield. (2014). Retrieved 10th June 2014, from http://www.seeedstudio.com/wiki/CAN-BUS_Shield

CAN-drivers. (n.d.). *can-drivers.txt: CAN netrowrk drivers.* Retrieved 11th July 2014, from https://gitorious.org/linux-can/can-modules/source/24eb8254863f936a129ec873f3209e516c2453a1:Documentation/networking/can/can-drivers.txt

can.txt. (n.d.). *can.txt: Readme file for the controller area network protocol family (aks SocketCAN.* Retrieved 11th July 2014, from https://www.kernel.org/doc/Documentation/networking/can.txt

Castillejo, P., Martínez, J.-F., López, L., & Rubio, G. (2013). An internet of things approach for managing smart services provided by wearable devices. *International Journal of Distributed Sensor Networks*, *2013*, 9. Retrieved from http://dx.doi.org/10.1155/2013/190813

Chamberlain, A., Martiñez-Reyes, F., Jacobs, R., Watkins, M., & Shackford, R. (2013). Them and us: An indoor pervasive gaming experience. *Entertainment Computing*, *4*(1), 1-9. Retrieved 1st November 2013, from http://www.academia.edu/attachments/30482670/download_file

Chang, C., Liang, M., Kou, H., & Si, Z. (2010). A review of encryption storage. *Information Technology Journal*, *9*(7), 1517-1520. Retrieved 12th September 2013, from http://scialert.net/abstract/?doi=itj.2010.1517.1520 doi: 10.3923/itj.2010.1517.1520

Charette, R. N. (2009). This car runs on code. *IEEE Spectrum*.

Chavez, M. L., Rosete, C. H., & Henriquez, F. R. (2005). Achieving confidentiality security service for CAN. In *Proceedings. 15th international conference on electronics, communications and computers, CONIELECOMP 2005.* (p. 166-170).

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., … Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th usenix conference on security* (p. 6-6). Berkeley, CA, USA: USENIX Association. Retrieved 10th August 2013, from http://dl.acm.org/citation.cfm?id=2028067.2028073

CiA. (n.d.). *Controller area network (CAN).* Retrieved 9th September 2013, from http://www.can-cia.org/index.php?id=can

CircuitCo CAN. (n.d.). *CircuitCo:CAN bus cape rev A.* elinux.org. Retrieved 10th June 2014, from http://elinux.org/CircuitCo:CAN_Bus_Cape_RevA

CircuitCo: CAN. (n.d.). *CircuitCo:CAN bus cape rev B.* elinux.org. Retrieved 10th June 2014, from http://elinux.org/CircuitCo:CAN_Bus_Cape_RevB

Cloud9 IDE. (n.d.). *Cloud9 ide: Revolutionary features, delivered.* Retrieved 17th June 2014, from https://c9.io/site/features/

Coley, G. (2014). *BeagleBone Black system reference manual, revision b* (Tech. Rep.). Beagleboard.org. Retrieved 5th April 2014, from https://github.com/CircuitCo/BeagleBone-Black/blob/rev_b/BBB_SRM.pdf?raw=true

Cook, J., Kolmanovsky, I., McNamara, D., Nelson, E., & Prasad, K. (2007). Control, computing and communications: Technologies for the twenty-first century model T. *Proceedings of the IEEE*, *95*(2), 334-355. doi: 10.1109/JPROC.2006.888384

Corrigan, S. (2008). *Introduction to the controller area network (CAN)* (Application Report - SLOA101A). Dallas, TX, USA: Texas Instruments. Retrieved 28th October 2013, from http://www.ti.com/lit/an/sloa101a/sloa101a.pdf

Dabacan, M. (2013). *Analog discovery technical reference manual* (Tech. Rep.). Pullman, WA, USA: Digilent Inc. Retrieved 5th July 2014, from http://www.digilentinc.com/Data/Products/ANALOG-DISCOVERY/Discovery_TRM_RevB_1.pdf

Dang, Q. (2012). *Recommendation for applications using approved hash algorithms* (NIST Special Publication 800-107, Rev 1). Gaithersburb, MD, USA: National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved 28th July 2014, from http://csrc.nist.gov/publications/nistpubs/800-107-rev1/sp800-107-rev1.pdf

Dardanelli, A., Maggi, F., Tanelli, M., Zanero, S., Savaresi, S., Kochanek, R., & Holz, T. (2013). A security layer for smartphone-to-vehicle communication over Bluetooth. *Embedded Systems Letters, IEEE*, *5*(3), 34-37. doi: 10.1109/LES.2013.2264594

Debian. (2014). *Introduction to debian: reasons to choose Debian.* Retrieved 17th June 2014, from https://www.debian.org/intro/why_debian

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94-103. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=84635968&site=ehost-live

Di Natale, M. (2008, October). Understanding and using the Controller Area

Network. *Lecture Notes*. Retrieved 5th July 2014, from http://www6.in.tum.de/pub/Main/TeachingWs2013MSE/CANbus.pdf

Dierks, T., & Allen, C. (1999). *The TLS protocol, version 1.0* (Memo No. RFC2246). Internet Engineering Task Force: IETF Network Working Group. Retrieved 5th November 2013, from http://tools.ietf.org/html/rfc2246

Donohue, B. (2013). Hacking the modern automobile. *Kaspersky*. Retrieved 8th January 2014, from http://blog.kaspersky.com/car-hacking/

Drinic, M., & Kirovski, D. (2004). A hardware-software platform for intrusion prevention. In *Proceedings of the 37th annual IEEE/ACM international symposium on microarchitecture* (p. 233-242). Washington, DC, USA: IEEE Computer Society. Retrieved 8th August 2013, from http://dx.doi.org/10.1109/MICRO.2004.2

Drolia, U., Wang, Z., Pant, Y., & Mangharam, R. (2011). Autoplug: An automotive test-bed for electronic controller unit testing and verification. In *Intelligent transportation systems (itsc), 2011 14th international ieee conference on* (p. 1187-1192). doi: 10.1109/ITSC.2011.6083139

Easttom, W. (2011). *Computer security fundamentals* (2nd ed.). Que Publishing Company.

Ebert, C., & Salecker, J. (2009). Guest editors' introduction: Embedded software technologies and trends. *Software, IEEE*, *26*(3), 14-18. doi: 10.1109/MS.2009.70

Embedded Systems Academy. (n.d.). *CAN best & worst case calculator.* Retrieved 20th June 2014, from http://www.esacademy.com/en/library/calculators/can-best-and-worst-case-calculator.html

Ergen, S. C. (2004). *Zigbee/ieee 802.15. 4 summary.*

Etschberger, C. (2003). CANopen: An introduction. *EE Times*. Retrieved 14th January 2014, from http://www.eetimes.com/document.asp?doc_id=1275818

Farkas, K. I., Heidemann, J., & Iftode, L. (2006). Intelligent transportation and pervasive computing. *IEEE Pervasive Computing Magazine*, *5*(4), 18-19. Retrieved 5th October 2013, from http://www.isi.edu/~johnh/PAPERS/Farkas06a.html ((Special issue guest editors))

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: design principles and practical applications*. Indianapolis, IN: Wiley Pub., inc.

Ferreira, J., Fonseca, J., & Lopes, J. (2012). Wireless vehicular communications for automatic incident detection and recovery. In *10th portugese conference on automatic control, CONTROLO'2012* (p. 339-344). Retrieved 6th August 2013, from http://www.apca.pt/publicacoes/6/paper85.pdf

Fessi, B., Hamdi, M., Benabdallah, S., & Boudriga, N. (2007). A decisional framework system for computer network intrusion detection. *European Journal of Operational Research*, *177*(3), 1824-1838.

FIPS PUB 200. (2006). *Minimum security requirements for federal information and information systems* (Federal Information Processing Standards Publication). Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST). Retrieved 29th December 2013, from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Fluhrer, S. R., Mantin, I., & Shamir, A. (2001). Weaknesses in the key scheduling algorithm of rc4. In *Revised papers from the 8th annual international workshop on selected areas in cryptography* (pp. 1–24). London, UK, UK: Springer-Verlag. Retrieved from http://dl.acm.org/citation.cfm?id=646557.694759

Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *NDSS 2011, proceedings of the network and distributed system security symposium.* Retrieved 12th January 2014, from https://eprint.iacr.org/2010/332.pdf

Franqueira, V. N. L., & Wieringa, R. J. (2012). Role-based access control in retrospect. *Computer*, *45*(6), 81-88.

Freier, A., Karlton, P., & Kocher, P. (2011). *The secure sockets layer (ssl) protocol version 3.0* (Historical Record No. RFC6101). Internet Engineering Task Force (IETF). Retrieved from http://tools.ietf.org/html/rfc6101

Gebotys, C. H. (2009). *Security in embedded devices.* Springer.

Goodman, S. E., & Lin, H. S. (Eds.). (2007). *Toward a safer and more secure cyberspace.* Committee on Improving Cybersecurity Research in the United States, National Research Council. The National Academies Press. Retrieved 16th August 2013, from http://www.nap.edu/openbook.php?record_id=11925

Gourdin, B., Soman, C., Bojinov, H., & Bursztein, E. (2011). Toward secure embedded web interfaces. In *Proceedings of the 20th USENIX conference on security* (pp. 2–2). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2028067.2028069

Greenberg, A. (2013). Hackers reveal nasty new car attacks – with me behind the wheel (video). *Forbes.* Retrieved 8th January 2014, from http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

Groll, A., & Ruland, C. (2009). Secure and authentic communication on existing in-vehicle networks. In *Intelligent vehicles symposium, 2009 IEEE* (p. 1093-1097).

Groza, B., & Murvay, P.-S. (2011a). Higher layer authentication for broadcast in Controller Area Networks. In *6th international conference on security and cryptography, SECRYPT 2011* (p. 188-197). SciTePress.

Groza, B., & Murvay, P.-S. (2012). *Broadcast authentication in a low speed controller area network.* Retrieved 28th July 2013, from http://www.aut.upt.ro/~bgroza/Papers/CANAut.pdf

Groza, B., & Murvay, S. (2011b). Secure broadcast with one-time signatures in Controller Area Networks. In *Availability, reliability and security (ARES), 2011 sixth international conference on* (p. 371-376). IEEE.

Groza, B., & Murvay, S. (2013). Efficient protocols for secure broadcast in controller area networks. *Industrial Informatics, IEEE Transactions on, 9*(4), 2034-2042. doi: 10.1109/TII.2013.2239301

Groza, B., Murvay, S., van Herrewege, A., & Verbauwhede, I. (2012). LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks. In *The 11th international conference on cryptology and network security, CANS.*

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

Hamilton, M. D., Tunstall, M., Popovici, E. M., & Marnane, W. P. (2008). Side channel analysis of an automotive microprocessor. In *IET Irish Signal and Systems Conference (ISSC).* Retrieved 12th September 2013, from `http://www.cs.bris.ac.uk/home/tunstall/papers/BTPM08.pdf`

Hammerschmidt, C. (2012). Flexray not dead, chip vendors claim. *EE Times.* Retrieved 12th January 2014, from `http://www.electronics-eetimes.com/en/flexray-not-dead-chip-vendors-claim.html?cmp_id=7&news_id=222914480`

Han, K., Divya Potluri, S., & Shin, K. (2013). On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. In *Cyber-physical systems (ICCPS), 2013 ACM/IEEE international conference on* (p. 160-169). doi: 10.1109/ICCPS.2013.6604010

Hartkopp, O., Reuber, C., & Schilling, R. (2012). MaCAN - Message Authenticated CAN. In *10th ESCAR conference on embedded security in cars.*

Hartwich, F., & Bosch, R. (2012). CAN with flexible data-rate. In *Proceedings of the 13th iCC* (pp. 14-1 – 14-9). Retrieved 14th January 2014, from `http://www.can-cia.org/fileadmin/cia/files/icc/13/hartwich.pdf`

Hazem, A., & Fahmy, H. A. H. (2012). LCAP - a lightweight CAN authentication protocol for securing in-vehicle networks. In *10th ESCAR conference on embedded security in cars.*

Herrewege, A. V., Singelee, D., & Verbauwhede, I. (2011). CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. *ECRYPT Workshop on Lightweight Cryptography 2011*.

Hoppe, T., Kiltz, S., & Dittmann, J. (2009). Automotive IT-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats. In *Proceedings of the 28th international conference on computer safety, reliability, and security* (p. 145-158). Berlin, Heidelberg: Springer-Verlag. Retrieved from http://dx.doi.org/10.1007/978-3-642-04468-7_13

Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN networks – practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety*, *96*(1), 11-25.

Hubaux, J.-P., Čapkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security and Privacy*, *2*(3), 49-55. Retrieved from http://dx.doi.org/10.1109/MSP.2004.26

Idrees, M. S., Schweppe, H., Roudier, Y., Wolf, M., Scheuermann, D., & Henniger, O. (2011). Secure automotive on-board protocols: A case of over-the-air firmware updates. In *Proceedings of the third international conference on communication technologies for vehicles* (pp. 224–238). Berlin, Heidelberg: Springer-Verlag. Retrieved from http://dl.acm.org/citation.cfm?id=1987310.1987333

Ingalls, R. (n.d.). *Sockets tutorial.* Course Notes. Retrieved 10th July 2014, from http://www.cs.rpi.edu/~moorthy/Courses/os98/Pgms/socket.html

ISO/IEC 7498-1. (1994). *Information technology - Open Systems Interconnection - basic reference model: The basic model* (Tech. Rep.). Geneva, Switzerland: The International Organization for Standardization (ISO) & the International Electrotechnical Commissionn (IEC). Retrieved 29th December 2013, from http://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf

ITU-T X.800. (1991). *Security architecture for open systems interconnection for ccitt applications* (Tech. Rep.). Geneva, Switzerland: The International Telegraph and Telephone Consultative Committee (ITTCC). Retrieved 29th December 2013, from http://handle.itu.int/11.1002/1000/3102

Kalinsky, D. (2012). Security fundamentals for embedded software. *Embedded Systems Design Magazine*, 12-18. Retrieved 9th August 2013, from http://www.kalinskyassociates.com/Wpaper13.html

Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., … others (2008). Secure vehicular communication systems: implementation, performance, and research challenges. *Communications Magazine, IEEE*, *46*(11), 110-118.

Kelly, H. (2013). The five scariest hacks we saw last week. *CNN*. Retrieved 8th January 2014, from `http://edition.cnn.com/2013/08/05/tech/mobile/five-hacks/`

Kermani, M., Zhang, M., Raghunathan, A., & Jha, N. (2013). Emerging frontiers in embedded security. In *VLSI design and 2013 12th international conference on embedded systems (VLSID), 2013 26th international conference on* (p. 203-208). doi: 10.1109/VLSID.2013.222

Khoh, S. B., & McLaughlin, R. T. (1994). Autos carry the CAN controller area network [CAN] for industrial applications. *Assembly Automation*, *14*(1), 17 - 19. doi: 10.1108/EUM0000000004198

Kim, T.-H., Bauer, L., Newsome, J., Perrig, A., & Walker, J. (2011). Access right assignment mechanisms for secure home networks. *Communications and Networks, Journal of*, *13*(2), 175-186. doi: 10.1109/JCN.2011.6157417

Kissel, R. L. (2013). *Glossary of key information security terms.* (NIST Interagency/Internal Report (NISTIR) No. 7298rev2). U.S. Department of Commerce: National Institute of Standards and Technology. Retrieved 20th December 2013, from `http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810`

Kleberger, P., Olovsson, T., & Jonsson, E. (2011). Security aspects of the in-vehicle network in the connected car. In *Intelligent vehicles symposium (IV), 2011 IEEE* (p. 528-533).

Kleidermacher, D., & Kleidermacher, M. (2012). *Embedded systems security: Practical methods for safe and secure software and systems development.* Oxford, UK: Newnes.

Klein, A. (2008, September). Attacks on the rc4 stream cipher. *Des. Codes Cryptography*, *48*(3), 269–286. Retrieved from `http://dx.doi.org/10.1007/s10623-008-9206-6` doi: 10.1007/s10623-008-9206-6

Kleine-Budde, M. (2012). Socketcan - the official CAN API of the Linux kernel.

In *Proceedings of the 13th international can conference (icc)* (p. 05.17-05.22). Nuremberg, Germany: CAN in Automation (CiA). Retrieved from http://www.can-cia.org/fileadmin/cia/files/icc/13/kleine-budde.pdf

Kleine-Budde, M. (2013). Socketcan - the official CAN API of the Linux kernel. In *Proceedings of the automotive linux summit.* Linux Foundation. Retrieved from http://events.linuxfoundation.org/sites/events/files/slides/elce2013-Kleine-Budde.pdf

Kochanek, R., Dardanelli, A., Maggi, F., Zanero, S., Tanelli, M., Savaresi, S., & Holz, T. (n.d.). *Secure integration of mobile devices for automotive services.* Retrieved 6th August 2013, from http://maggi.cc/static/assets/publications/2012_kochanek_dardanelli_maggi_zanero_tanelli_savaresi_holz_autosec_tr/paper.pdf

Koopman, P. (2004). Embedded system security. *Computer*, *37*(7), 95-97.

Koopman, P. (2013). *The FlexRay protocol.* Retrieved 12th January 2014, from http://www.ece.cmu.edu/~ece649/lectures/23_flexray.pdf

Koopman, P., & Szilagyi, C. (2013). Integrity in embedded control networks. *Security & Privacy, IEEE*, *11*(3), 61-63.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., … Savage, S. (2010). Experimental security analysis of a modern automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy* (p. 447-462). Washington, DC, USA: IEEE Computer Society. Retrieved from http://dx.doi.org/10.1109/SP.2010.34

Krawczyk, H. (2001). *The order of encryption and authentication for protecting communications (or: how secure is ssl?).* Cryptology ePrint Archive, Report 2001/045. Retrieved 16th July 2014, from http://eprint.iacr.org/

Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. *Artificial Intelligence Review*, *34*(4), 369-387. Retrieved from http://dx.doi.org/10.1007/s10462-010-9179-5

Kuo, C.-C., Lin, J.-N., Wu, S.-H., Cho, C.-H., Chu, Y.-H., & Tsai, F.-D. (2013).

An in-vehicle communication scheme for multi-system integration. In *Wireless and pervasive computing (ISWPC), 2013 international symposium on* (p. 1-4). doi: 10.1109/ISWPC.2013.6707427

Kurose, J. F., & Ross, K. W. (2013). *Computer networking: a top-down approach* (6th International ed.). Upper Saddle River, N.J; Harlow: Pearson Education.

Laird, J. (2013). The rise of car hacking: In-car technology has led to thieves remotely taking over our vehicles. *The Independent, UK*. Retrieved 8th January 2014, from `http://www.independent.co.uk/life-style/motoring/features/the-rise-of-car-hacking-incar-technology-has-led-to-thieves-remotely-taking-over-our-vehicles-8825012.html`

Lampson, B. (2009). Privacy and security: Usable security: How to get it. *Commun. ACM*, *52*(11), 25–27. Retrieved from `http://doi.acm.org/10.1145/1592761.1592773` doi: 10.1145/1592761.1592773

Larson, U. E., Nilsson, D. K., & Jonsson, E. (2008). An approach to specification-based attack detection for in-vehicle networks. In *Intelligent vehicles symposium, 2008 ieee* (p. 220-225).

Leavitt, N. (2010). Researchers fight to keep implanted medical devices safe from hackers. *Computer*, *43*(8), 11-14. doi: 10.1109/MC.2010.237

Leonard, M. (2014, February). How to choose the right platform: Raspberry Pi or BeagleBone Black. *Make:*. Retrieved 5th April 2014, from `http://makezine.com/magazine/how-to-choose-the-right-platform-raspberry-pi-or-beaglebone-black/`

Lukasiewycz, M., Steinhorst, S., Andalam, S., Sagstetter, F., Waszecki, P., Chang, W., … Chakraborty, S. (2013). System architecture and software design for electric vehicles. In *Proceedings of the 50th annual design automation conference* (pp. 95:1–95:6). New York, NY, USA: ACM. Retrieved from `http://doi.acm.org/10.1145/2463209.2488852` doi: 10.1145/2463209.2488852

Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, *35*(3), 934-941.

Marques, R., Navet, N., & Simonot-Lion, F. (2005). Configuration of in-vehicle embedded systems under real-time constraints. In *Emerging technologies and factory automation, 2005. etfa 2005. 10th ieee conference on* (Vol. 1, p. 8 pp.-414). doi: 10.1109/ETFA.2005.1612554

Martin, C. (n.d.). *What is IPS and how intrusion prevention system works.* Retrieved 30th December 2013, from http://www.aboutonlinetips.com/what-is-ips-and-how-intrusion-prevention-system-works/

Mason, S. (2012). Vehicle remote keyless entry systems and engine immobilisers: Do not believe the insurer that this technology is perfect. *Computer Law & Security Review*, *28*(2), 195 - 200. Retrieved from http://www.sciencedirect.com/science/article/pii/S0267364912000222 doi: http://dx.doi.org/10.1016/j.clsr.2012.01.004

Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K., & Oishi, K. (2012). A method of preventing unauthorized data transmission in controller area network. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th* (p. 1-5).

McLaughlin, R. (n.d.). *Controller area network (CAN): understanding the basics and its role in automotive diagnostics.* Retrieved 19th September 2013, from http://www.warwickcontrol.com/ata/Infobackup_and_library/Basicbus.pdf

McMillan, R. (2010). Car hackers can kill brakes, engine, and more. *TechHive: Security*. Retrieved 8th January 2014, from http://www.techhive.com/article/196293/car_hackers_can_kill_brakes_engine_and_more.html

MCP2515. (2012). *Microchip mcp2515: stand-alone CAN controller with SPI interface* (Data Sheet & Application Note). Chandler, AZ, USA: Microchip Technology Inc. Retrieved 25th March 2014, from http://ww1.microchip.com/downloads/en/DeviceDoc/21801G.pdf

MCP2551. (2010). *Microchip mcp2515: high-speed CAN transceiver* (Data Sheet & Application Note). Chandler, AZ, USA: Microchip Technology Inc.

Retrieved 5th July 2014, from
http://ww1.microchip.com/downloads/en/DeviceDoc/21667f.pdf

Miller, C., & Valasek, C. (2013). *Adventures in automotive networks and control units* (Tech. Rep.). Seattle, WA, USA: IOActive Labs Research. Retrieved 8th January 2014, from http://illmatics.com/car_hacking.pdf

Mironov, I. (2002). (not so) random shuffles of rc4. In M. Yung (Ed.), *Advances in cryptology âĂŤ crypto 2002* (Vol. 2442, p. 304-319). Springer Berlin Heidelberg. Retrieved from
http://dx.doi.org/10.1007/3-540-45708-9_20 doi: 10.1007/3-540-45708-9_20

Muter, M., Groll, A., & Freiling, F. C. (2010). A structured approach to anomaly detection for in-vehicle networks. In *Information assurance and security (ias), 2010 sixth international conference on* (p. 92-98).

National Instruments. (2013). *Embedded systems outlook 2013: significant trends, opportunities, and challenges impacting today's embedded system design teams.* (Tech. Rep.). Austin, TX, USA: National Instruments (NI). Retrieved 2nd January 2014, from http://www.ni.com/pdf/products/us/351334C_01_08604_ESO_Outlook.pdf

Navet, N., & Perrault, H. (2012). CAN in automotive applications: A look forward. In *Proceedings of the 13th iCC* (pp. 14-1 – 14-9). Retrieved 14th January 2014, from
http://www.can-cia.org/fileadmin/cia/files/icc/13/navet.pdf

Navet, N., Song, Y., Simonot-Lion, F., & Wilwert, C. (2005). Trends in automotive communication systems. *Proceedings of the IEEE*, *93*(6), 1204-1223. doi: 10.1109/JPROC.2005.849725

Nilsson, D., & Larson, U. (2009). A defense-in-depth approach to securing the wireless vehicle infrastructure. *Journal of Networks*, *4*(7). Retrieved from http://ojs.academypublisher.com/index.php/jnw/article/view/0407552564

Nilsson, D. K., Larson, U. E., & Jonsson, E. (2008a). Efficient in-vehicle delayed data authentication based on compound message authentication codes. In *Vehicular technology conference, 2008. vtc 2008-fall. ieee 68th* (p. 1-5).

Nilsson, D. K., Larson, U. E., & Jonsson, E. (2008b). Low-cost key management for hierarchical wireless vehicle networks. In *Intelligent vehicles symposium, 2008 ieee* (p. 476-481).

Node.js. (2010). *Node.js.* Retrieved 20th June 2014, from http://nodejs.org/

NRC. (2002). *Cybersecurity today and tomorrow: Pay now or pay later* (Tech. Rep.). Washington, D.C., USA: Computer Science and Telecommunications Board, National Research Board. Retrieved 16th August 2013, from http://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay-now-or-pay-later-national-research-council-2002.pdf

NSA. (n.d.). *Defense in depth: a practical strategy for achieving Information Assurance in today's highly networked environments* (Tech. Rep.). Fort Meade, MD, USA: National Security Agency. Retrieved 16th August 2013, from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Oguma, H., Yoshioka, A., Nishikawa, M., Shigetomi, R., Otsuka, A., & Imai, H. (2008). New attestation based security architecture for in-vehicle communication. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (p. 1-6).

OpenSSL. (n.d.). *EVP.* Retrieved 26th July 2014, from https://www.openssl.org/docs/crypto/evp.html

Oshana, R., & Kraeling, M. (2013). *Software engineering for embedded systems: Methods, practical techniques, and applications.* Newnes, an imprint of Elsevier Science and Technology Books, Inc.

Paar, C., & Weimerskirch, A. (2007). Embedded security in a pervasive world. *Information Security Technical Report*, *12*(3), 155-161.

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., … Hubaux, J.-P. (2008). Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, *46*(11), 100-109.

Papadimitratos, P., & Hubaux, J.-P. (2008). Report on the "secure vehicular communications: Results and challenges ahead" workshop. *SIGMOBILE Mob. Comput. Commun. Rev.*, *12*(2), 53–64. Retrieved from http://doi.acm.org.remote.library.dcu.ie/10.1145/1394555.1394567 doi:

10.1145/1394555.1394567

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277-290. Retrieved from http://www.emeraldinsight.com/journals.htm?issn=0968-5227 doi: 10.1108/09685221011079199

Patel, H. B., Patel, R. S., & Patel, J. A. (2011). Approach of data security in local network using distributed firewalls. *International Journal of P2P Network Trends and Technology*, *11*(3), 26-29. Retrieved 10th August 2013, from http://www.ijpttjournal.org/volume-1/issue-3/IJPTT-V1I3P405.pdf

Paul, N., Kohno, T., & Klonoff, D. C. (2011). A review of the security of insulin pump infusion systems. *Journal of Diabetes Science and Technology*, *5*(6), 1557-1562. Retrieved 12th January 2014, from http://dst.sagepub.com/content/5/6/1557.abstract doi: 10.1177/193229681100500632

PICAN. (n.d.). *PICAN CAN-Bus board for raspberry pi.* Retrieved 10th June 2014, from http://skpang.co.uk/catalog/pican-canbus-board-for-raspberry-pi-p-1196.html

Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. *Wireless Communications, IEEE*, *13*(5), 8-15. doi: 10.1109/WC-M.2006.250352

Reynolds, F. (2008). Whither Bluetooth? *IEEE Pervasive Computing*, *7*(3), 6-8. doi: http://doi.ieeecomputersociety.org/10.1109/MPRV.2008.63

Richards, P. (2002). *A CAN physical layer discussion* (Application Note: AN228). Chandler, AZ, USA: Microchip Technology Inc. Retrieved 19th September 2013, from http://ww1.microchip.com/downloads/en/AppNotes/00228a.pdf

Richardson, R. (2011). *CSI computer crime and security survey* (Tech. Rep.). GoCSI.com: Computer Security Institute. Retrieved 16th August 2013, from http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf

Rivas, D. A., Barceló-Ordinas, J. M., Zapata, M. G., & Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. *Journal of Network and Computer Applications*, *34*(6), 1942-1955.

Roemer, M., & Kramer, A. (2010). *The intelligent car: embedded systems, a success story for the German job market* (Tech. Rep.). Dusseldorf, Germany: A.T. Kearney Embedded Systems Study. Retrieved 29th December 2013, from `https://www.austria.atkearney.com/documents/3709812/3710822/BIP_The_Intelligent_Car.pdf/5346cd61-779e-4114-adc9-1e1de1afc798`

Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., … Seskar, I. (2010). Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *Proceedings of the 19th USENIX Conference on Security* (pp. 21–21). Berkeley, CA, USA: USENIX Association. Retrieved from `http://dl.acm.org/citation.cfm?id=1929820.1929848`

RSA. (2000). *RSA laboratories' frequently asked questions about today's cryptography.* Cambridge, MA, USA. Retrieved 25th September 2013, from `http://www.emc.com/emc-plus/rsa-labs/historical/crypto-faq.htm`

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *Communications Magazine, IEEE*, *32*(9), 40-48.

Schweppe, H., & Roudier, Y. (2012). Security and privacy for in-vehicle networks. In *Vehicular communications, sensing, and computing (vcsc), 2012 ieee 1st international workshop on* (p. 12-17). doi: 10.1109/VCSC.2012.6281235

Serpanos, D. N., & Voyiatzis, A. G. (2013). Security challenges in embedded systems. *ACM Trans. Embed. Comput. Syst.*, *12*(1), 66:1–66:10. doi: 10.1145/2435227.2435262

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*(4), 656-715. Retrieved from `http://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy`

_Systems;http://www.alcatel-lucent.com/bstj/vol28-1949/articles/bstj28-4-656.pdf;http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

Shi, W. V., & Zhou, M. (2012). Body sensors applied in pacemakers: A survey. *Sensors Journal, IEEE*, *12*(6), 1817-1827. doi: 10.1109/JSEN.2011.2177256

SN65HVD230. (2011). *Sn65hvd230 3.3V CAN transceivers* (Data Sheet & Application Note). Dallas, TX, USA: Texas Instruments. Retrieved 20th March 2014, from http://www.ti.com/lit/ds/symlink/sn65hvd230.pdf

SocketCAN.png. (2009). *File: Socketcan.png.* Wikimedia Commons. Retrieved 28th June 2014, from http://commons.wikimedia.org/wiki/File:Socketcan.png

Stajano, F. (2002). *Security for ubiquitous computing.* John Wiley & Sons, Ltd.

Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.). Upper Saddle River, NJ, USA: Prentice Hall Press.

Stallings, W., & Brown, L. (2011). *Computer security: Principles and practice* (2nd ed.). Upper Saddle River, NJ, USA: Prentice Hall Press.

Stapko, T. (2007). *Practical embedded security: Building secure resource-constrained systems.* Newnes, an imprint of Elsevier Science and Technology Books, Inc.

Strang, T., & Röckl, M. (2008). *Vehicle networks lecture: Controller area network (CAN).* Retrieved 19th September 2013, from http://www.sti-innsbruck.at/sites/default/files/courses/fileadmin/documents/vn-ws0809/02-VN-CAN.pdf

Stubblefield, A., Ioannidis, J., & Rubin, A. D. (2004). A key recovery attack on the 802.11b wired equivalent privacy protocol (wep). *ACM Trans.Inf.Syst.Secur.*, *7*(2), 319-332. Retrieved from http://doi.acm.org/10.1145/996943.996948

Studer, A., Bai, F., Bellur, B., & Perrig, A. (2009). Flexible, extensible, and efficient VANET authentication. *Communications and Networks, Journal of*, *11*(6), 574-588.

Studnia, I., Nicomette, V., Éric Alata, Deswarte, Y., Kaâniche, M., & Laarouchi, Y. (2013). A survey of security threats and protection mechanisms in embedded automotive networks. In *Proceedings of the 2nd Workshop on Open Resilient human-aware Cyber-physical Systems (WORCS-2013), co-located with the IEEE/IFIP Annual Symposium on Dependable Systems and Networks (DSN-2013)* (p. 1-12).

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaaniche, M., & Laarouchi, Y. (2013). Security of embedded automotive networks: state of the art and a research proposal. In M. ROY (Ed.), *Proceedings of Workshop CARS (2nd Workshop on Critical Automotive applications : Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security* (p. NA).

Szilagyi, C., & Koopman, P. (2008). A flexible approach to embedded network multicast authentication. In *2nd workshop on embedded systems security (WESS).*

Tanenbaum, A. S. (2007). *Modern operating systems* (3rd ed.). Upper Saddle River, NJ, USA: Prentice Hall Press.

TCG. (2012). *Secure embedded platforms with trusted computing: automotive and other systems in the Internet of Things must be protected* (White Paper). Beaverton, OR, USA: Trusted Computing Group (TCG). Retrieved 12th August 2013, from http://www.trustedcomputinggroup.org/files/static_page_files/3057DF77-1A4B-B294-D033A50B2D91B70B/Secure%20Embedded%20Platforms%20with%20Trusted%20Computing%20Automotive%20and%20Other%20Systems%20in%20the%20Internet%20of%20Things%20Must%20Be%20Protected.pdf

Thompson, H. H., Whittaker, J. A., & Andrews, M. (2004). Intrusion detection: Perspectives on the insider threat. *Computer Fraud & Security*, *2004*(1), 13-15.

TI BBB. (n.d.). *BeagleBone Black development board.* Dallas, TX, USA. Retrieved 5th April 2014, from http://www.ti.com/tool/beaglebk?DCMP=PPC_Google_TI&k_clickid=2cb2d12f-c026-0fe8-13c5-000022de8fb9#TechnicalDocuments

Tindell, K., Burns, A., & Wellings, A. (1995). Calculating controller area network (CAN) message response times. *Control Engineering Practice*, *3*(8), 1163 - 1169. Retrieved from `http://www.sciencedirect.com/science/article/pii/0967066195001128` doi: http://dx.doi.org/10.1016/0967-0661(95)00112-8

Todorov, D. (2007). *Mechanics of user identification and authentication.* Boston, MA, USA: Auerbach Publications.

Tower Technologies. (n.d.). *TT3201 CAN Cape user's manual.* Retrieved 18th April 2014, from `http://www.towertech.it/en/products/hardware/tt3201-can-cape/manual/`

Tsai, C.-S., Tsai, K.-S., & Hsu, M.-T. (2012). An implementation of the enhanced-CAN BUS network connection in CAR real-time embedded software system. In *Control, automation and systems (ICCAS), 2012 12th international conference on* (p. 277-283).

Turley, J. (2003). *Motoring with microprocessors.*

van der Linde, E., & Hancke, G. P. (2011). An investigation of bluetooth mergence with ultra wideband. *Ad Hoc Networks*, *9*(5), 852-863.

Verendel, V., Nilsson, D. K., Larson, U. E., & Jonsson, E. (2008). An approach to using honeypots in in-vehicle networks. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th* (p. 1-5). IEEE.

Wan, J., Zou, C., Ullah, S., Lai, C.-F., Zhou, M., & Wang, X. (2013). Cloud-enabled wireless body area networks for pervasive healthcare. *Network, IEEE*, *27*(5), 56-61. doi: 10.1109/MNET.2013.6616116

Wang, J. (2009). *Computer network security: Theory and practice* (1st ed.). Springer.

Watterson, C. (2012). *Control area network (CAN) implementation guide* (Application Note AN-1123). Norwood, MA, USA: Analog Devices, Inc. Retrieved 19th September 2013, from `http://www.analog.com/static/imported-files/application_notes/AN-1123.pdf`

Waveshare. (2011). *Schematic prints of CAN_Board.schDoc.* Retrieved 1st July 2014, from `http://www.wvshare.com/downloads/accBoard/SN65HVD230-CAN-Board.7z`

Wolf, M. (2009). *Security engineering for vehicular IT systems: improving the trustworthiness and dependability of automotive it applications.* Springer.

Wolf, M., Weimerskirch, A., & Paar, C. (2006). Secure in-vehicle communication. In K. Lemke, C. Paar, & M. Wolf (Eds.), (p. 95-109). Springer Berlin Heidelberg. Retrieved 01 September 2013, from http://dx.doi.org/10.1007/3-540-28428-1_6

Wolf, M., Weimerskirch, A., Paar, C., & Bluetooth, M. (2004). Security in automotive bus systems. In *Proceedings of the workshop on embedded security in cars (ESCAR)'04.* Retrieved 11th September 2013, from http://www.weika.eu/papers/WolfEtAl_SecureBus.pdf

Wolf, M., Weimerskirch, A., & Wollinger, T. (2007). State of the art: Embedding security in vehicles. *Eurasip Journal on Embedded Systems*, *2007*, 1-17.

Wyglinski, A., Huang, X., Padir, T., Lai, L., Eisenbarth, T., & Venkatasubramanian, K. (2013). Security of autonomous systems employing embedded computing and sensors. *Micro, IEEE*, *33*(1), 80-86. doi: 10.1109/MM.2013.18

Zhang, L., Wu, Q., Solanas, A., & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. *Vehicular Technology, IEEE Transactions on*, *59*(4), 1606-1617.

Zhao, Y. (2002). Telematics: Safe and fun driving. *IEEE Intelligent Systems*, *17*(1), 10-14. Retrieved from http://dx.doi.org/10.1109/5254.988442

Ziermann, T., Wildermann, S., & Teich, J. (2009). Can+: A new backward-compatible controller area network (CAN) protocol with up to 16× higher data rates. In *Design, automation & test in europe conference & exhibition, 2009. (DATE '09).* (p. 1088-1093).