ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

A Survey - Security Layer For Smartphone -To-Vehicle Communication Over Bluetooth

Yogita Jadhav[1], Ganesh Wayal[2]

PG Scholar, Dept. of CE, Mukesh Patel School of Technology Management & Engineering, Shirpur,India[1]
Assistant Professor, Dept. of IT, Mukesh Patel School of Technology Management & Engineering, Shirpur, India[2]

ABSTRACT:Modern vehicles are increasingly being interconnected with computer systems, which collect information both from vehicular sources and Internet services Vulnerabilities likes improper validation, exposure, and randomness. These vulnerabilities include device address validation, invalid states, and exposed keys. Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP) and other attack of falsification of information are major findings. In this article I come up solution that allows a Smartphone to establish a secure session layer over an insecure radio connection, which provides additional security guarantees regardless of the security mechanisms. Hierarchically distributed control system architecture which integrates a smartphone with classical embedded systems, and an ad-hoc, end-to-end security layer is designed to demonstrate how a smartphone can interact securely with a modern vehicle without requiring modifications to the existing in vehicle network As a result, the entire application layer is transparently secured with implementation of RSA algorithm for encryption.

Keywords: Gateway ECU, CAN Bus, Automotive systems, Embedded Architecture, Security, Smartphone, Two-wheeled vehicles.

I. INTRODUCTION

A. GATEWAY ELECTRONIC CONTROL UNIT (ECU) [5]

A gateway Electronic Control Unit (ECU) is a central network interconnecting system to link various field buses in a vehicle. A gateway ECU is used to interconnect Controller Area Network (CAN) and Local Interconnect Network (LIN) field buses for Low Price Vehicles (LPVs)[8]. A gateway ECU is required for addressing the communication and network challenges in today's vehicles. Various existing commercial gateway ECU, and derive the specification for a gateway ECU suitable for LPVs. Gateway ECU is designed based on specification and implemented using PIC microcontroller and line transceivers for interconnecting LIN and CAN buses[6]. The designed gateway ECU has been successfully validated using two other nodes– one node with LIN and another with CAN networks. Gateway ECU has optimal functionality and is cost effective solution for LPV segments. The trends in automotive networks and electronics show that the LPV needs to have only CAN and LIN networks in next one to two decades[19]. In short, gateway ECU has optimal balance between functionality and cost, and is best suitable for LPVs[7]. In now a days, each new function was implemented as a standalone ECU, which is a sub-system composed of a microcontroller and a set of sensors and actuators. The evolution of automotive electronics since 1960 was tremendous starting from simple ignition control to Xby-wire technology by 2010 [2].As the electronics increased, the Need for functions to be distributed over several ECUs and the need for information exchanges among them have been evolved. The different performance requirements throughout a vehicle, as well as competition among the companies in automotive industry, have led to the design of a large number of communication networks. A gateway is required to manage all these in vehicle networks and messages effectively. Network gateway is a device or a piece of software in a computer that forwards and routes data packets along networks. A possible gateway concept in a LPV is depicted in Fig. 1.This focuses to design gateway ECU to interconnect LIN and CAN networks.

B . Secure Session Layer[20]

In Secure Session Layer the first stage is to sets up an end-to-end trusted relationship between both application layers (i.e., on the mobile device and on the ECU). Due to the constraints of the scenario (e.g., distribution of the mobile application through app stores, connectivity capabilities of the ECU), user do not assume any precomputed, static credentials or cryptographic keys on the mobile device, nor use a public-key infrastructure on the ECU: Only the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

vehicle's owner is able to initiate the first stage by enabling the one-off authorization procedure on the vehicle's side[32]. For instance, this procedure can be enabled by pushing a button only reachable using the vehicle key. A classic PIN-based procedure is not always feasible, due to the limited input capabilities on the ECU side (e.g., absence of keypads). Within a short time span the ECU accepts a mobile device's identity and the user receives the identity information of the ECU, respectively. The second stage ensures that the real-time communication requirements are meet[33]. It implements a symmetric cryptographic scheme that establishes a secure communication session. The symmetric session key is derived from the long-term secret exchanged during the first stage, plus some random data generated on the mobile device[12].

C. CAN-Bluetooth Gateway Layer[18][19]

The CAN-Bluetooth gateway filters and sends the information over the CAN bus according to the database of accessible information. The gateway also implements a SPP to communicate according to the Bluetooth protocol [20]. The measurements of the vehicle are translated into notifications, and the commands are turned into commands to VCU. At the gateway. level, a critical alert may also be recognized on the CAN and then sent to the upper level[11].

D. The Smartphone Layer[13]

From a computational point of view, the smartphone represents the core of the system. The mobile device is characterized by the presence of an operating system that allows the multi tasking of the processes (e.g., Windows Mobile, Symbian, and Google Android). The software for the VEDE system may be developed according to the appropriate platform and to the operating system[17]. The interface between the mobile device and the gateway is implemented with the SPP over Bluetooth. The interface between the smartphone and the helmet is provided by the HFP or, alternatively, by the HSP over Bluetooth. The software on the smartphone translates the notification from the gateway into a stream of audio data (voice synthesis). It also turns the speaker data from the helmet into a command to the gateway (speech recognition). The smartphone also manages the communication to and from the web server (remote point) according to the HTTP protocol (natively embedded in the mobile) [16].

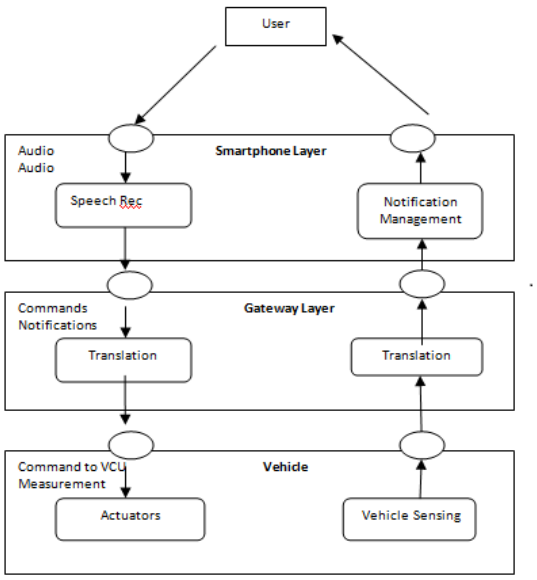

Fig 1: Software architecture representing the driver-to-vehicle interaction

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

II. SECURITY LAYER FOR SMARTPHONE-TO-VEHICLE COMMUNICATION OVER BLUETOOTH USING RSA

Modern vehicles are increasingly being interconnected with computer systems, which collect information both from vehicular sources and Internet services. Unfortunately, this creates a non negligible attack surface, which extends when vehicles are partly operated *via* smartphones. Bluetooth is by design a peer-to-peer network technology and typically lacks centralized administration and security enforcement infrastructure. The Bluetooth specification is very complex and includes support for over two dozen diverse voice and data "profiles" or services. Because of these complexities, Bluetooth is particularly susceptible to a diverse set of security vulnerabilities. Publicly documented Bluetooth attacks involve identity detection, location tracking, denial of service, unintended control and access of data and voice channels, and unauthorized device control and data access[30]. .Vulnerabilities were found as a result of improper validation, exposure, and randomness. These vulnerabilities include device address validation, invalid states, and exposed keys. Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP). The attacks are based on the falsification of information sent during the input/output capabilities exchange and also the fact that the security of the protocol is likely to be limited by the capabilities of the least powerful or the least secure device type[4].

A. Public Key Cryptocraphy Using RSA For Encryption

This algorithm RSA is used for public key encryption and it generate digital signature for encryption [24]Alggorithm works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key[25]. It is theoretically possible but extremely difficult to generate the private key from the public key. DSA is faster at signing than RSA, but RSA is faster during the verification phase, since authentication requires both phases the difference doesn't matter[26]. As I said above DSA can only be used for authentication while RSA can be used for both authentication and to encrypt a message. However, SSH only uses the keys for authentication, so again the difference doesn't matter[27][28].

The RSA algorithm steps for key generation are

1. Generate two different primes p and q
2. Calculate the modulus $n = p \times q$
3. Calculate the $f(n) = (p - 1) \times (q - 1)$
4. Choose public exponent an integer e such that $1 < e < f(n)$ And $gcd(f(n), e) = 1$
5. Select the private exponent a value for d such that $d = e\text{-}1 \bmod f(n)$
6. Public Key = [e, n]
7. Private Key = [d, n]

III. LITERATURE SURVEY

I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser,W. Trappe, and I. Seskar [1] have review on Tire Pressure Monitoring System (TPMS) used for Monitors tire-pressure in real time, alerts drivers if underinflated, increase safety and fuel economy and it's misuse for car tracking and security over it by reverse engineering, Eavesdrop capability, spoofing validation.

S.Checkoway, D.McCoy, B.Kantor, D.Anderson, H.Shacham, S.Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno[2] have propoes experimental analysis of external attack surface of a modern automobile used for discover that remote exploitation on short range and long range wireless network and come up with the result that short range network is less secure than long range wireless networkon the basis of parameters like direct and indirect physical layer .

A. Dardanelli, M. Tanelli, B. Picasso, S. Savaresi, O. di Tanna, and M. Santucci [4] have proposed a novel, spatially distributed and hierarchical control architecture that is capable of regulating the battery state of charge by imposing a desired discharge rate considering two State Of Charge(SoC).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

C.Spelta,V.Manzoni,A.Corti,A.Goggi, and S. M. Savaresi [5] have proposed system consists of a vehicle-to-driver and a vehicle-to-environment communication mechanism, which is based on a smartphone core and on a wireless Bluetooth medium. The system is focused to increase the safety level of a motorcycle and it is constituted by a vehicle with a CAN bus, a compact embedded electronic unit implementing a CAN-to-Bluetooth gateway, a smartphone and a Bluetooth helmet.

B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall [9] have proposed design called SlyFi is nearly as efficient as existing schemes such as WPA for discovery , link setup, and data delivery despite its heightened protections;transmission requires only symmetric key encryption and reception requires a table lookup followed by symmetric key decryption. Experiments using our implementation on Atheros 802.11 drivers show that SlyFi can discover and associate with networks faster than 802.11 using WPA-PSK.

A. Juels and J. Brainard. [11] have proposed cryptoghaphical countermeasure named client puzzle protocol in oppose of connection depletion attacks which is a denial – of – service attacks. In it when server faced attacks a it distributes small cryptographical puzzle to client.After solving that puzzle correctly server provide service to client.

Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga [12] have proposed simulation model over By looking at the packet interarrival times in three representative MAC protocols, S-MAC, LMAC and B-MAC against jamming attacks are based on realistic assumptions and come up with result that more jammer motes have greater jamming effect, and the more sensor nodes a jammer mote has as neighbors, the sooner the jammer mote can synchronize with the S-MAC/LMAC schedule.

L. Lazos, S. Liu, and M. Krunz [13] have proposed new security metrics that extends the ability of the opposer to reject access to the control channel, and the total delay gained in reestablishing the control channel. They also propose a randomized distributed design that allows nodes to establish a new control channel using frequency hopping. This method from classic frequency hopping in that no two nodes share the same hopping sequence, thus mitigating the impact of node compromise.

G. Lin and G. Noubir [14] have proposed the scheme to jamming of data protocols, such as IP, over WLAN. Jammer used on existing WLAN an adversary can successfully jam data packets at a very low energy cost. attacks allow a set of opponent nodes diffusion over an area to prevent communication, partition an ad hoc network, or force packets to be routed over adversary chosen paths.

X. Liu, G. Noubir, and R. Sundaram [15] have proposed SPREAD - a novel new assortment vision to provide scheme against cross-layer denial of service attack. SPREAD respite on a mechanism hopping technique, which can be seen as a multi-layer extension of the frequency-hopping technique. It apply to game-theoretic framework for modeling the interaction of the communicating nodes and the adversaries and analyze the proposed approach..

Y. Liu, P. Ning, H. Dai, and A. Liu.[16] have proposed Randomized Differential DSSS (RD-DSSS) scheme to gain anti-jamming broadcast communication without shared keys. RD-DSSS encodes each bit of data using the correlation of unpredictable spreading codes. It is used to defeat reactive jamming attacks, RDDSSS uses multiple spreading code sequences to spread each message and rearranges the spread output before transmitting it.

R. C. Merkle [17] have review on use of select a key over open communications channels in way that communications security can be maintained. It forces any enemy to expend an amount of work which increases as the square of the work required of the two communicants to select the key. The method provides a logically new kind of protection against the passive eavesdropper**.**

G. Noubir and G. Lin [18] have reviewed scheme of jamming of data protocols, such as IP, over WLAN and a concatenated code that is simple to decode and can maintain a low Frame Error Rate (FER) under a jamming effort ratio **.**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

C. Perkins, E. Belding-Royer, and S. Das [20] have proposed Ad-hoc On Demand DistanceVector Routing (AODV) a novel algorithm for the operation of Mobile Ad-Hoc Networks(MANET). Each Mobile node act as a specialized router and routes are obtained on demand with little or no reliance or periodic advertisements This routing algorithm is quite suitable for a dynamic self starting network as required by users wishing to utilize ad-hoc networks.

C. Popper, M. Strasser, and S.Capkun [21] have proposed a solution called Uncoordinated DSSS (UDSSS) which able to organize spread-spectrum anti-jamming broadcast communication without the need of shared secrets. It is applicable to broadcast scenarios in which receivers hold an authentic public key of the sender but do not share a secret key with it. UDSSS can handle an unlimited amount of receivers while being secure against malicious receivers.

R. Rivest [22] have proposed new scheme of encryption for block cipher named all-or-nothing encryption.It decrypt whole ciphertext before determining even one message block.They implement scheme using package transform which follows ordinary codebook encryption parallely .It provide protection against selected-plaintext and related-message attacks**.**

R. Rivest, A. Shamir, and D. Wagner [23] have proposed scheme of trusted agents to solve problem "timed release crypto" where the goal of the scheme is to encrypt a message so that it can not be decrypted by any one I overcome problems of ensuring that the agents are trustworthy secret sharing.It depend on the amount and nature of the hardware used to solve the problem as well as the parallelizability of the computational problem being solved.

M. Strasser, C. P¨opper, and S. ˇCapkun [29] have proposed the vision of solving problem of FHSS and DSSS encryption by indroducing Uncoordinated Frequency Hopping (UFH).It is spread-spectrum anti-jamming technique that does not rely on secret keys.

P. Tague, M. Li, and R. Poovendran [31] have proposed sheme over the problems denial of service attack by the use of random key distribution to hide the location of control channels in time and frequency. It evaluate performance metrics of resilience to control channel jamming, identification of compromised users, and delay due to jamming as a function of the number of compromised users.

P. Tague, M. Li, and R [32] have proposed a framework for control channel access schemes using the random assignment of cryptographic keys to hide the location of control channels. It evaluate metrics to quantify the probabilistic availability of service under control channel jamming by malicious or compromised users and show that the availability of service degrades gracefully as the number of colluding insiders or compromised users increases.

IV. CONCLUSION AND FUTURE WORK

In this article I studied Vulnerabilities likes improper validation, exposure, and randomness in bluetooth. These vulnerabilities include device address validation, invalid states, and exposed keys. Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP) and the attacks are based on the falsification of information are major findings. I come up with solution that allows a Smartphone to establish a secure session layer over an insecure radio connection, which provides additional security guarantees regardless of the security mechanisms. Hierarchically distributed control system architecture which integrates a smartphone with classical embedded systems, and an ad-hoc, end-to-end security layer is designed to demonstrate how a smartphone can interact securely with a modern vehicle without requiring modifications to the existing in vehicle network As a result, the entire application layer is transparently secured with implementation of RSA algorithm for encryption.

REFERENCES .

1. I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser,W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in car wireless networks: A tire pressure monitoring system case study," in Proc. 19th USENIX Conf. Security, Berkeley, CA, USA, 2010, pp. 21–21.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

2. 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," in Proc. 20th USENIX Conf. Security, Berkeley, CA, USA, 2011,.

3. F. Stajano, Security for Ubiquitous Computing. Hoboken, NJ, USA:Wile, 2002.

4. A. Dardanelli, M. Tanelli, B. Picasso, S. Savaresi, O. di Tanna, and M. Santucci, "A smartphone-in-the-loop active state-of-charge manager for electric vehicles," IEEE ASME Trans. Mechatron., vol. 17, no. 3, pp. 454–463, 2012.

5. C.Spelta,V.Manzoni,A.Corti,A.Goggi, and S. M. Savaresi, "Smartphone-based vehicle-to-driver/environment interaction system for motorcycles," IEEE Embed. Systems Lett., vol. 2, no. 2, pp. 39–42, Jun.2010.

6. Microchip Technology Inc., 16-bit dsPIC® Digital Signal Controllers.

7. NIST Special Publication 800-121 Revision 1, Guide to Bluetooth Se- K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

8. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

9. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

10. IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

11. A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.

12. Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

13. L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

14. G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.

15. X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536–2540, 2007.

16. Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.

17. R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.

18. G. Noubir and G. Lin. Poster : Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review,7(3):29–30, 2003.

19. OPNET. OPNETtm modeler 14.5. http://www.opnet.com/.

20. C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc on demand distance vector (AODV) routing. Internet RFCs, 2003.

21. C. Popper, M. Strasser, and S. Capkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

22. R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.

23. R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. Massachusetts Institute of Technology, 1996.

24. B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, 2007.

25. SciEngines. Break DES in less than a single day. http://www.sciengines.com, 2010.

26. M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

27. D. Stinson. Something about all or nothing (transforms). Designs,Codes and Cryptography, 22(2):133–138, 2001.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

28. D. Stinson. Cryptography: theory and practice. CRC press, 2006.

29. M. Strasser, C. P¨opper, and S. ˇCapkun. Efficient uncoordinated fhss anti-jamming communication. In Proceedings of MobiHoc, pages 207–218, 2009.

30. M. Strasser, C. P¨opper, S. ˇCapkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In Proceedings of IEEE Symposium on Security and Privacy, 2008.

31. P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of PIMRC, 2007.

32. P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.

BIOGRAPHY

Yogita Jadhav is a M.Tech student of the Computer Engineering at the University of NMIMS, Shirpur. She received her B.E degree in the IT Department at the University of Pune, Nashik in 2012 . Her current research interests include Smartphone to Smartphone communication in wireless ad-hoc and sensor networks and attacks and defense mechanisms.

Ganesh Wayal is Assistant Professor in IT Department at the University of NMIMS, Shirpur .He received his M.Tech degree in Computer Technology and Application from University of RGPV, Bhopal in 2009. He received his B.E degree in Computer Science and Engineering at the university PCST, Bhopal in 2006. His current research interest include Mobile ad-hoc network with BlackBerry.