자율주행차 메모리 보안 취약점 분석

홍석현 [1], 김태욱 [2], 백재원 [3], 조영필 [4]
[1] 한양대학교 미래자동차-SW 융합전공 석박통합과정
[2] 한양대학교 미래자동차-SW 융합전공 석사과정
[3] 한양대학교 정보보안학과 석사과정
[4] 한양대학교 컴퓨터소프트웨어학과 교수

ghazard8572@hanyang.ac.kr, qkenr7895@hanyang.ac.kr, qor291@hanyang.ac.kr, ypcho@hanyang.ac.kr

Analysis of Memory Security Vulnerability in Autonomous Vehicles

Seok-Hyun Hong[1], Tae-Wook Kim[2], Jae-Won Baek[3], Yeong-Pil Cho[4]
[1]Dept. of Computer and Software (Automotive-Computer Convergence), Han-Yang University
[2]Dept. of Computer and Software (Automotive-Computer Convergence), Han-Yang University
[3]Dept. of Information Security, Han-Yang University
[4]Dept. of Computer Science, Han-Yang University

요 약

자율주행차가 제공하는 새로운 시장과 경쟁력, 인력 및 시간 절약, 교통 체증 문제 해결 등의 장점을 다루고, UN 사이버 보안 법률에 따른 자율주행차의 기술적인 요구사항을 준수해야 한다. 하지만 자율주행차에 대한 기술적인 요구사항을 준수하는 것으로는 모든 사이버 공격에 대해서 막을 수 없다. 자율주행차의 법적 요구사항과 사이버 보안 위협에 대처하는 방법을 다룬다. 특히 RTOS(Real Time OS)와 같은 실시간 시스템에 매우 위험할 수 있는 DRAM(Dynamic Random Access Memory)에 대한 로우해머링 공격 기법에 대해 분석하고 로우해머링에 대한 보안 방법을 제시한다. 그리고 자율 주행 시스템의 안전과 신뢰성을 보장하기 위해 하드웨어 기반 또는 소프트웨어 기반 방어 기술을 소개하고 있다.

1. 서론

자율주행차가 개발되고 상용화됨에 따라 자율주행차를 제조하는 기업들을 이를 통해 경쟁력을 갖출 수 있고, 새로운 비즈니스 모델을 창출 할 수 있다. 또한 운전에 필요한 인력과 시간을 절약한다. 이를 통해 교통 체증 문제를 해결하고 시간과 비용을 절감할 수 있다. 하지만 이러한 새로운 시장에 대한 법 제정도 있었는데 유엔 사이버 보안 법률은 전세계적인 컴퓨터 보안 표준을 수립하고, 사이버 공격을 방지하기 위한 국제적인 협력을 촉진하기 위해 노력하고 있다. 특히 자율주행차와 같은 차량에서 사용되는 소프트웨어와 하드웨어의 보안을 강화하기 위한 기술적인 요구사항을 제시하고 있다. 또한 법률은 자동차 제조업체 및 관련 기업이 자체적으로 보안 위협에 대응하기 위한 계획과 절차를 마련하도록 권고하고 있다. 이를 통하여 자율주행차를 제조업체들에게 법적인 기준을 제시하여 보다 안전하고 신뢰성 있는 자율 주행차를 개발할 수 있도록 돕는다. 하지만 이러한 노력에도 불구하고 자율주행차는 외부 공격 및 사이버 공격에 취약하다. 따라서 자율주행차 메모리 보안은 자율주행차 시스템 전체의 보안을 유지하는데 필수적이다. 메모리 존재하는 취약점은 해커들이 시스템을 공격하고, 제어권을 탈취하는데 이용될 수 있다. 이를 방지하기 위해서는 자율주행차에 대한 메모리 보안이 강화되어야 한다. 본 논문에서는 기존 방어 방식으로는 막지 못하는 로우해머링(Row Hammering)공격과 로우해머링을 방어방법을 소개한다.

2. 자율주행차 공격 유형 및 보안 기술 표준화

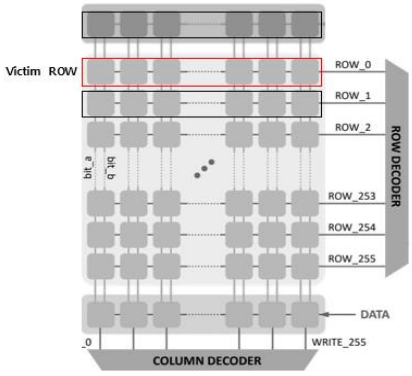
2.1 자율주행차 보안 기술 표준화

UN Regulations 155[1]와 156[2]는 자율주행차를 개발하고 생산하는 제조업체들에게 법적인 기준을 제시하여 보다 안전하고 신뢰성 있는 자율주행차를 개발할

수 있도록 장려한다. 또한, 이 규격은 자율주행차의 글로벌한 수요를 충족시키기 위해 국제적인 표준화를 촉진한다. UN-R155 은 자율주행차를 위한 "Automated Lane Keeping Systems"의 기술적 요구사항을 규정하고 있다. 이 규격은 자동차가 도로 상황을 모니터링하고 차선 유지 기능을 수행할 수 있도록 하는 기술적인 요구사항을 제시한다. UN-R156 은 자율주행차를 위한 "Automated Emergency Braking Systems"의 기술적 요구사항을 규정하고 있다. 이 규격은 자동차가 도로 상황을 모니터링하고 위험한 상황에서 자동으로 제동을 걸어 안전한 차간 거리를 유지할 수 있도록 하는 기술적인 요구사항을 설명한다. 또한 차량 외부 통신 보안[3]은 차량간 V2X 보안의 경우 IEEE 1609.2 및 CAMP VSC3 표준 기반으로 기술개발이 이루어져 현재 국내, 국제적으로 테스트베드를 구축하여 실증하는 단계에 있다.

이처럼 많은 자율주행차 관련 보안 기술이 표준화되고 있다. 하지만 이러한 표준에도 자율주행차에서 실시간으로 중요한 정보를 저장하는 DRAM 은 로우해머링에 취약하기 때문에 자동차 제조사와 보안 전문가들은 계속해서 보안 기술을 개발하고 보안에 대한 대처책을 지속해서 강구할 필요가 있다.

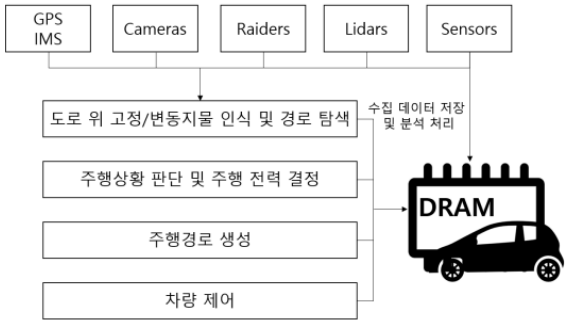
2.2 로우 해머링 공격 방법



(그림 1) TRRespass 로우해머링

TRRespass[4]는 일부 DRAM 칩에서 발생하는 잡음 현상을 악용하는 공격 기술이다. TRRespass 는 실제로 메모리 셀을 직접적으로 공격하는 것이 아니라, DRAM 칩의 신호선에서 발생하는 잡음을 이용한다. 로우해머링 공격은 이러한 셀들 사이의경계를 무너뜨려 하나의 셀을 연속적으로 공격한다. TRRespass 공격은 일부 DRAM 칩에서만 발생할 수 있는 문제이며, 이러한 칩들은 이전에 로우해머링 공격에 취약하다는 것이 알려져 있다. ECCPLOIT[5]는 특정 DRAM 구성에서만 사용 가능한 로우해머링 공격 기법이다. 이 기법을 이용하면 일부 DRAM 셀이 간섭을 받아 비트가 뒤바뀔 수 있다. 그러나 ECCPLOIT 은 TRRespass 보다 더 낮은 성공률을 보이고, 실제 세상에서는 매우 드물게 발생한다. SpecHammer[6]는 CPU 의 분기 예측 기능을 이용하여 DRAM 에 로우해머링 공격을 수행하는 기술이지만 일부 CPU 모델에 한정된다. 하지만 이러한 로우해머링 공격은 자율주행차에서 발생하면 심각한 위험이 될 수 있다.

3. 자율주행차 메모리 보안의 필요성



(그림 2) 자율주행차의 DRAM 을 통한 저장 및 분석 방법

자율주행차에서 DRAM 은 데이터를 처리하고 저장하여 자율주행 시스템의 성능을 향상시키는 데 중요한 역할을 한다. 그리고 ECU(Electronic Control Unit)는 자동차의 전자 제어 시스템을 관리하고 조작하여 자율주행 시스템의 안정성을 유지한다. DRAM 은 주로 차량 내부에서 데이터를 저장하고 처리하는 데 사용된다. 자율주행 시스템에서는 카메라, 레이더 및 센서 등에서 수집한 데이터를 처리하고 저장하는 데 사용된다. RTOS[7]는 주로 실시간 시스템에서 사용되는 운영 체제이며, 이러한 시스템은 일반적으로 높은 안정성과 신뢰성이 요구된다. 하지만 RTOS 에서 로우해머링 공격은 매우 심각한 보안 위협으로 작용할 수 있다. 로우해머링으로 인해 DRAM 에 저장된 데이터가 변경될 경우, 자율주행차의 센서 데이터나 제어 명령이 오류를 일으켜 사고가 발생할 수 있다. 따라서 메모리 보안에 대한 충분한 대책이 필요하다.

4. 자율주행차 메모리 보안 방법

메모리 보안은 자율주행차에서 저장된 정보가 잘못되어 잘못된 판단을 내릴 수 있는 잠재적인 보안 위협에서 보호할 수 있다. 다음은 로우해머링과 같은 메모리 공격을 방어하는 방법이다.

- **Error Correcting Code (ECC) Memory**: ECC 메모리는 DRAM 에서 발생할 수 있는 에러를 감지하고 수정할 수 있는 기술이다. 이 기술은 DRAM 에서의 로우해머링에 대한 대처책 중 하나다.
- **Address Space Layout Randomization (ASLR)[8]**: ASLR 은 메모리에 할당되는 주소를 무작위로 지정하여 악성 코드가 메모리 주소를 예측하는 것을 어렵게 만든다. 이를 통해 로우해머링 공격을 방지할 수 있다.
- **소프트웨어 수준 방어 기술**: Mathril[9]은 로우해머링

공격을 방어하기 위해 DRAM 의 주소 매핑 기능을 사용한다. 이를 통해 DRAM 의 데이터와 메타데이터를 더욱 안전하게 보호할 수 있다. 이 방법은 하드웨어를 수정하지 않고 소프트웨어적으로 구현이 되어 기존 시스템과 호환성이 높다.

- **운영체제 수준 방어 기술**: 운영체제에서는 메모리를 DRAM 을 TRR(Target Row Refresh)가 적용되어 특정 행에 대해 주기적으로 새로고침하여 로우해머링을 방어하는 기술이 있다.

- **하드웨어 수준 방어 기술**: DRAM 메모리 내부에 로우해머링 공격에 대한 자가 보호 기능을 내장하는 방법이 있다. Silver Bullet[10]은 로우해머링 공격에 취약한 bit line 을 자동으로 탐지하여 매번 다른 위치에 있는 bit line 으로 주소 매핑을 수행함으로써 공격을 방어한다.

하지만, 이러한 기술이 완전한 방어가 될 수는 없고 보안 위협은 계속해서 발전하기 때문에, 자동차 제조사와 보안 전문가들은 계속해서 보안 기술을 개발하고 업그레이드하며, 보안에 대한 대비책을 계속해서 추구해야 한다. 따라서, 자동차 제조사들은 지속적으로 보안 취약성을 모니터링하고 최신 보안 기술을 도입하여 보안 위협에서 자율주행차를 보호해야 한다.

5. 결론

자율주행차가 새로운 부가가치를 창출하는 시장으로 많은 제조사들이 비즈니스 모델을 창출하고 있다. 하지만 뒤따르는 책임으로 인하여 국제 자율주행차 관련 법안을 준수해야 하고 법을 제정할 수 없는 사이버 보안에 대해 대처를 해야 한다. 그 중 자율주행차에 저장 및 분석을 담당하고 있는 DRAM 은 로우해머링 공격에 취약하고 RTOS 인 자율주행차에 심각한 위험을 초래할 수 있다. 이에 따라 로우해머링에 대한 보안을 위해 메모리 액세스 패턴 변경, 로우해머링을 감지하는 소프트웨어 도구를 사용하는 등에 보안에 취약점을 대응책을 개발하고 지속적으로 보안 위협에 대해서 분석할 필요가 있다.

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기회평가원의 지원을 받아 수행된 연구임.(No.2020-0-01840, 스마트폰의 내부데이터 접근 및 보호 기술 분석)

참고문헌

[1] Un regulation no 155 – uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387],” Mar 2021.

[2] Un regulation no 156 – uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388],” Mar 2021.

[3] N. Jung-Chan, “Security trends for autonomous driving vehicle,” Feb. 2018.

[4] P. Frigo, E. Vannacc, H. Hassan, V. Van Der Veen, O. Mutlu, C. Giuffrida, H. Bos, and K. Razavi, “Trrespass: Exploiting the many sides of target row refresh,” in 2020 IEEE Symposium on Security and Privacy (SP), pp. 747–762, IEEE, 202

[5] L.Cojocar, K.Razavi,C.Giuffrida, and H.Bos, “Exploiting correcting codes: On the effectiveness of ecc memory against rowhammer attacks,” in 2019 IEEE Symposium on Security and Privacy (SP) , pp. 55–71, IEEE, 2019.

[6] Y.Tobah, A.Kwong, I.Kang, D.Genkin, and K.G.Shin, “Spechammer: Combining spectre and rowhammer for new speculative attacks,” in 2022 IEEE Symposium on Security and Privacy (SP) , pp. 681–698, IEEE, 2022.

[7] P. Hambarde, R. Varma, and S. Jha, “The survey of real time operating system: Rtos,” in 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, pp. 34–39, IEEE, 2014.

[8] V.Van der Veen, M.Lindorfer, Y.Fratantonio, H.Padmanabha Pillai, G.Vigna, C.Kruegel, H.Bos, and K. Razavi, “Guardion: Practical mitigation of dma-based rowhammer attacks on arm,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 15th International Conference, DIMVA 2018, Saclay, France, June 28–29, 2018, Proceedings 15, pp. 92–113, Springer, 2018.

[9] M.J.Kim, J.Park, Y.Park, W.Doh, N.Kim, T.J.Ham, J.W.Lee, and J. H. Ahn, “Mithril: Cooperative row hammer protection on commodity dram leveraging managed refresh,” in 2022 IEEE International Symposium on High-Performance Computer Architecture (HPCA) , pp. 1156–1169, IEEE, 2022.

[10] A.G.Ya˘glıkçı, J.S.Kim, F.Devaux, and O.Mutlu, “Security analysis of the silver bullet technique for rowhammer prevention,” arXiv preprint arXiv:2106.07084, 2021.