UNIVERSITY AT ALBANY
State University of New York

Cyber Security in Self Driving Cars

Tech Squad: Anthony Waldner, Olivia Chemmannure, Nick Faeth, Yilei Zhao, Safi Milien, Christopher Bracci

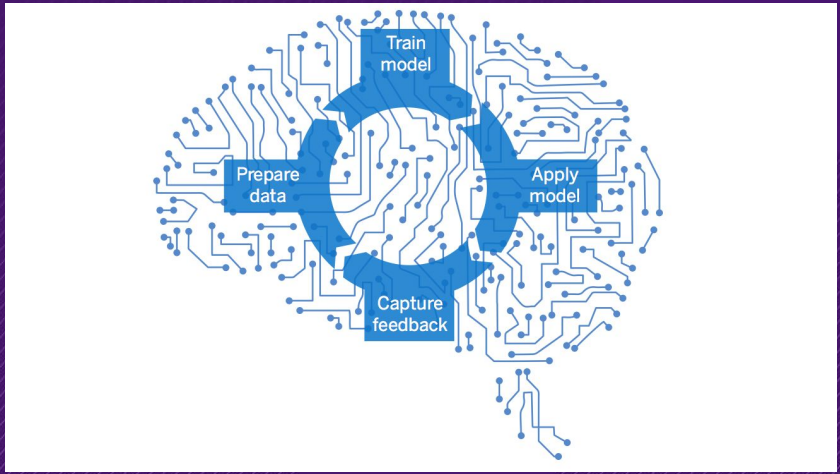
UNLEASH GREATNESS

UNIVERSITY AT ALBANY
State University of New York

UNLEASH
GREATNESS

Solutions Search - What are we focusing on?

- Machine Learning
- Simulation Testing
- Cloud Storage
- Code Reviewers/ Encryption
- Collaboration among manufacturing companies
- Firewall



Solution Mechanism - How do they work?

Machine Learning

- Object detection: the identification and the recognition of the objects classification
- Object localization: the prediction of where and the object is located and the ability to predict movement.

Algorithms

- Regression
- Pattern Recognition
  - Support vector machine - SVM
  - Histograms of Oriented Gradients - HOG
  - Principal Component Analysis - PCA
- Cluster
- Decision Matrix

Solution Mechanism - How do they work?

Simulation Testing

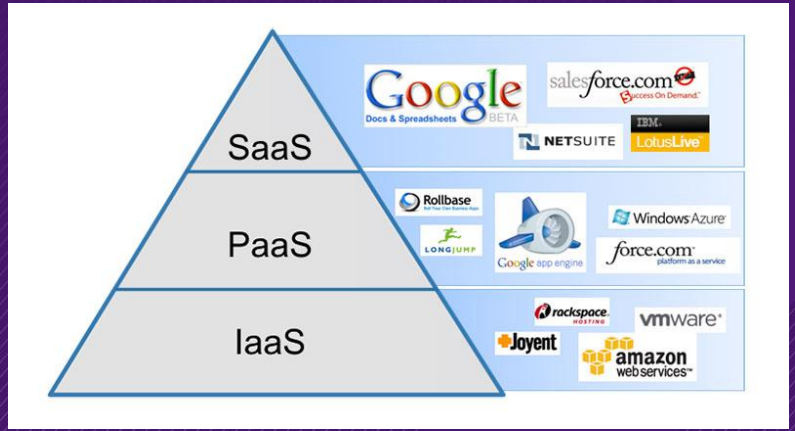
- Virtual Testing
  - Safety
  - Testing Exploits
  - Failure allows quick new data
- Quick learning
  - Machine learning
- Simulation is the framework
  - Creates quality of data

Solution Mechanism - How do they work?

Cloud Computing

Cloud Service Model

- Software as a Service (SaaS)
  - Google Docs
- Platform as a Service (PaaS)
  - Windows Azure
- Infrastructure as a Service (IaaS)
  - Joyent



Cloud Computing Integration

- Interact with Vehicles
- Storage
  - Set protocols
  - Records all data

Solution Mechanism - How do they work?

Code Reviewers

- Open source
  - Limits risk
- Open source for innovation
- Improvements
  - People can learn from other's methods making their own methods more efficient.

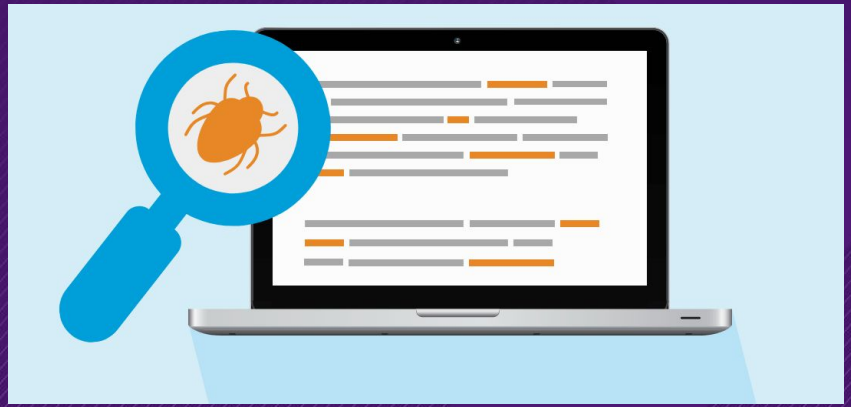
Encryption

- Secure and Safe
- Cyber Security
- Ties in with Firewall Protection

Solution Mechanism - How do they work?

Static Code Analysis

- Automated way of checking source code.
  - Efficient
  - Fast
- Helps catch things that might have been missed



Security Improvements

- Early Developments
- “Bug Hunts”
  - Code Exploits / Vulnerabilities

Solution Mechanism - How do they work?

Collaboration among manufacturing companies.

- Shared Technology between companies to prevent information breach.

Standard Safety Protocol

- Sharing protection and cybersecurity solutions
- Creates easy testing for vulnerabilities
- Reports of potential threats

Solution Mechanism - How do they work?

Firewall

AUTOSAR (Sectigo's Embedded Firewall)

- Embedded security system within automotive vehicles
- Prevent Cyber Attacks
  - Enforces Filtering rules
  - Detects anomalies
  - Identify Traffic

Solution Comparison - Technology Collaboration

- Technology and resources collaboration among manufacturing companies.
  - Advantage - Collaboration would mean better resources to develop a resilient technology that can secure the cars' infrastructure and keep hackers locked out.
  - Disadvantage - Each manufacturer may have a different coding system. It would give hackers an opportunity to exploit self-driving vehicles.

Solution Comparison - ML / Simulation Testing

- Machine Learning
  - Advantage - Identify & prevent unusual behavior
  - Disadvantage - Parameter selection, accuracy needs improvement, model selection restriction, additional methods for unbalanced dataset
- Simulation Testing
  - Advantage - Fast, more insights to underlying physics
  - Disadvantage - Expensive, don’t produce solutions

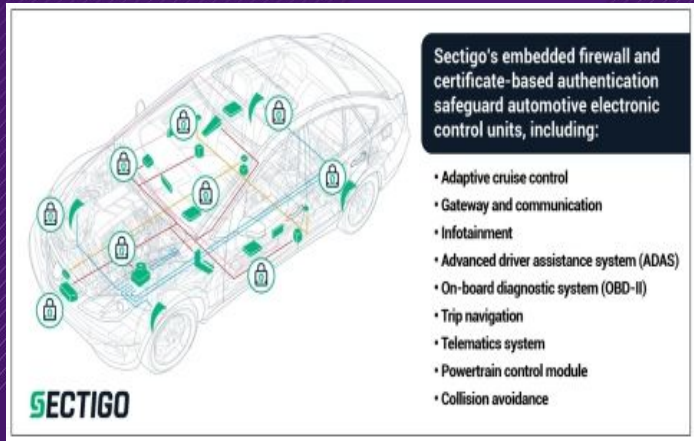
UNIVERSITY AT ALBANY
State University of New York

Solution Comparison - Cloud Storage / Encryption

- Cloud Storage
  - Advantage - Cheap, multiple layers of security
  - Disadvantage - Dependent on internet connection, no physical control of data
- Code Reviewers / Encryption
  - Advantage - Improves security/integrity of system software
  - Disadvantage - Information can't be highly encrypted w/o data delay

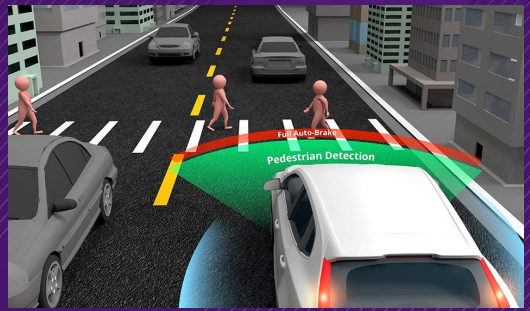
Solution Comparison - Firewall

- Firewall (Sectigo Embedded)
  - Advantage - Detects anomalies & identifies traffic variances to protect cars from network-based cyberattacks
  - Disadvantage - Controls all aspects of the vehicle



Solutions Integration - Machine Learning

- Our solution will involve the use of several potential solutions combined with machine learning being the main basis.
- Machine Learning with simulation testing will not only allow self-driving cars to test out how efficiently they are run, but also allows machine learning to map out what is going well and not so well.

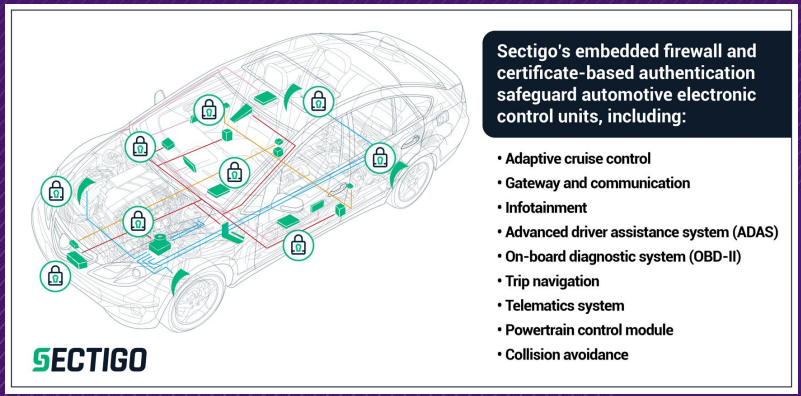


Solutions Integration - Cloud Storage

- The second main basis of our solution is the use of cloud storage.
- This is necessary for the protection of data within the cloud when it comes to the use of machine learning.
- This ensures the encryption and code review of data in order to prevent data from being compromised.

Solutions Integration - Firewall

- Although having an embedded firewall was one of the best options it has its shortcomings where it can interfere with other aspects of the car such as encryption or cloud storage access etc.



Thank You for your time! If you have any questions please let us know.

References

- N.P (2020, June 09). Modern machine Learning Algorithms: Strengths and weaknesses. Retrieved March 30, 2021, from https://elitedatascience.com/machine-learning-algorithms
- Mister, M. (2019, October 22). 10 advantages and disadvantages of cloud storage. Retrieved March 30, 2021, from https://www.promax.com/blog/10-advantages-and-disadvantages-of-cloud-storage

References (2)

- Colburn, L. (2019, December 18). Sectigo releases Embedded firewall to PROTECT automotive systems. Retrieved March 30, 2021, from https://www.businesswire.com/news/home/20191218005031/en/Sectigo-Releases-Embedded-Firewall-to-Protect-Automotive-Systems
- Grewal, J. (2020, April 27). Blockchain-powered autonomous automobiles can be the answer. Retrieved March 30, 2021, from https://www.ibm.com/blogs/blockchain/2020/04/blockchain-powered-autonomous-automobiles-can-be-the-answer/#:~:text=In%202019%2C%20IBM%20filed%20a,array%20of%20sensor%20IoT%20technologies

References (3)

- Bellairs, R. (2020, February 10). What is static analysis (static code analysis)? Retrieved March 30, 2021, from https://www.perforce.com/blog/sca/what-static-analysis
- Garg, A. (2020, July 24). Leveraging open source can be powerful for cybersecurity. Retrieved March 30, 2021, from https://securityintelligence.com/posts/open-source-cybersecurity/

References (4)

- Causevic, D. (2017, July 21). How machine learning can enhance cybersecurity for autonomous cars. Retrieved March 30, 2021, from https://www.toptal.com/insights/innovation/how-machine-learning-can-enhance-cybersecurity-for-autonomous-cars
- Ippolito, P. (2020, January 02). Future of cyber security for connected and autonomous vehicles. Retrieved March 30, 2021, from https://towardsdatascience.com/future-of-cyber-security-for-connected-and-autonomous-vehicles-4c553def6d50

References (5)

- Patel, R. (2020, March 04). What do self-driving cars have to do with machine learning for cybersecurity? Retrieved March 30, 2021, from https://securityboulevard.com/2018/05/what-do-self-driving-cars-have-to-do-with-machine-learning-for-cybersecurity/
- Stewart, E. (2019, May 17). Self-driving cars have to be safer than regular cars. the question is how much. Retrieved March 30, 2021, from https://www.vox.com/recode/2019/5/17/18564501/self-driving-car-morals-safety-tesla-waymo

References (6)

- Thing, V. L., & Wu, J. (2017, May 04). Autonomous vehicle security: A taxonomy of attacks and defences. Retrieved March 30, 2021, from https://ieeexplore.ieee.org/abstract/document/7917080
- Xu, W., Yan, C., Jia, W., Ji, X., & Liu, J. (2018, August 30). Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. Retrieved March 30, 2021, from https://ieeexplore.ieee.org/abstract/document/8451864

References (7)

- University, W. G. (2019, February 04). How cybersecurity drives self-driving car adoption. Retrieved March 30, 2021, from https://www.wgu.edu/blog/how-cybersecurity-drives-self-driving-car-adoption1812.html
- Elezaj, R. (2019, July 16). Autonomous Cars: Safety Opportunity or Cybersecurity Threat. Retrieved March 30, 2021, from https://www.machinedesign.com/mechanical-motion-systems/article/21837958/autonomous-cars-safety-opportunity-or-cybersecurity-threat

References (8)

- Bowles, J. (2019, May 23). Autonomous vehicles and the threat of hacking. Retrieved March 30, 2021, from https://www.cpomagazine.com/cyber-security/autonomous-vehicles-and-the-threat-of-hacking/
- N.P (N.D). Automotive cyber security course program. Retrieved April 13, 2021, from https://forms1.ieee.org/Automotive-Cyber-Security.html?LT=EA_WB_202010_LM_ACS_institute

References (9)

- Huntington, S. (2019, January 31). Car cloud computing integration, a new frontier for cloud. Retrieved April 13, 2021, from https://cloudacademy.com/blog/car-cloud-computing/
- Armerding, T. (2019, October 08). How to secure autonomous vehicles of the future, today: Synopsys. Retrieved April 13, 2021, from https://www.synopsys.com/blogs/software-security/secure-autonomous-vehicles/
- Eliot, L. (2020, December 28). Largest ever cyber hack provides vital lessons for self-driving cars. Retrieved April 13, 2021, from https://www.forbes.com/sites/lanceeliot/2021/12/29/largest-ever-cyber-hack-provides-vital-lessons-for-self-driving-cars/?sh=40d909ff715e

References (10)

- Williams, S. (2018, April 11). 20 real-world uses for blockchain technology. Retrieved April 13, 2021, from https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx
- Gupta, A. (2018, March 15). Machine Learning Algorithms in Autonomous Driving. Retrieved April 13, 2021, from https://iiot-world.com/artificial-intelligence-ml/machine-learning/machine-learning-algorithms-in-autonomous-driving/

References(11)

- N.P (N.D).Static analysis cracks the code to bug-free autonomous vehicles. Automotive World. (2019, March 14). https://www.automotiveworld.com/articles/static-analysis-cracks-the-code-to-bug-free-autonomous-vehicles/

References for Images

- SAP AI: Machine learning in oil & gas. (2017, May 06). Retrieved April 13, 2021, from https://blogs.sap.com/2017/05/06/sap-ai-machine-learning-in-oil-gas/
- Teaching ai self-driving cars to drive using simulations. (2020, November 28). Retrieved April 13, 2021, from https://www.nanalyze.com/2019/01/ai-self-driving-cars-simulations/
- Common cloud storage backup issues and possible solutions. (n.d.). Retrieved April 13, 2021, from http://www.thinkaxiom.com/axiology/common-cloud-storage-backup-issues-and-possible-solutions/