



# ottofence

## Automotive Cyber Security

**SIPL Projects July 2019 – an opening lecture**

**OttoFence Private**

## The “10 Topics ” pitch

1. Title
2. Problem/ Opportunity
3. Value Proposition
4. Undelaying magic
5. Business model
6. Go-To-Market plan
7. Competitive Analysis
8. Team
9. Financial projection and key metrics .....
10. Current status, Accomplishments to date, time line and use of funds .....

## CANBUS Automotive Networks The Situation & the Problem

- Modern vehicles rely on CANBUS networks for all their critical systems.
- CANBUS is a shared bus architecture. A single misbehaving node can effectively block all network communication say by generating a **Denial-Of-Service** attack.
- Possible Attack Vectors / Surface : Radio Receivers and OBD connectors
  - Infotainment ; Fleet Management; OnStar; V2V devices ; etc...
- For example it is possible to generate a Ransomware Attacks

[Cyber attack on Jeep 2015](#)      [Zombie Cars Scene The Fate of the Furious 2017](#)

[10TV news 1 Feb 2019 -Car Hacking by Argus](#)

[PenTestPartners Car Hack March 2019](#)

# OttoFence – Automotive Cyber Security

- Offering a small, effective & low cost CANBUS **firewall device**, identify and prevents Automotive Cyber-Attacks.



- initially designed for the **AFTER MARKET!**

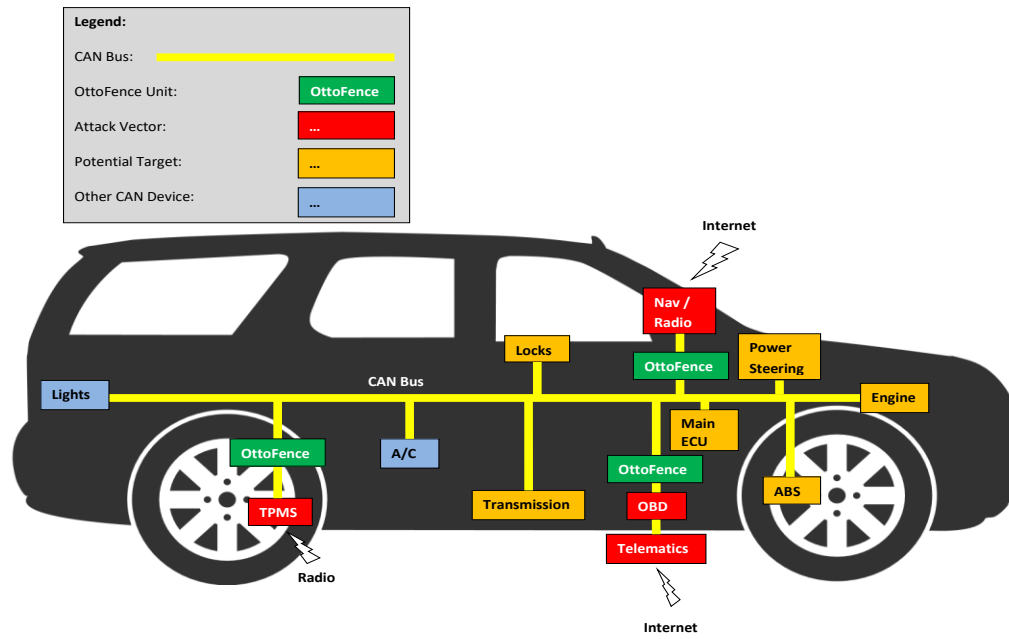
- Main investor **ADI SYSTEM**



- **ADI SYSTEMS** imports, markets, installs and provides a huge range of high level and sophisticated products as car accessories, multimedia, communication, protection and detection systems to enhance the driving experience.



### Vehicle CAN Diagram - OttoFence



OttoFence Private

# CANFence – Firewall

## “The Value Proposition”

- CANFence – A small HW device. A Firewall written as Embedded Software
- **Many Other** solutions are SW for integration at OEM ECU. It **does not solve** the after market security challenge
- High reliability HW and SW design to “Fail Safe”
  
- Consists of ‘**Rules**’ which are processed in-order
- ‘**Stateful**’ design: Past results can influence future messages
- Designed for **seamless** updating of rules at runtime

[OttoFence – Attack Demo](#)

[OttoFence – Attack & Defense](#)

[Attack Control Panel 1](#)

[Attack Control Panel 2](#)

[OF Cyber Attack Clip 1](#)

[OF Cyber Defense Clip 2](#)

[OF BotNet Attack clip3](#)

[OF Cyber BotNet Defense clip 4](#)

**Managed Over-The-Air Device**

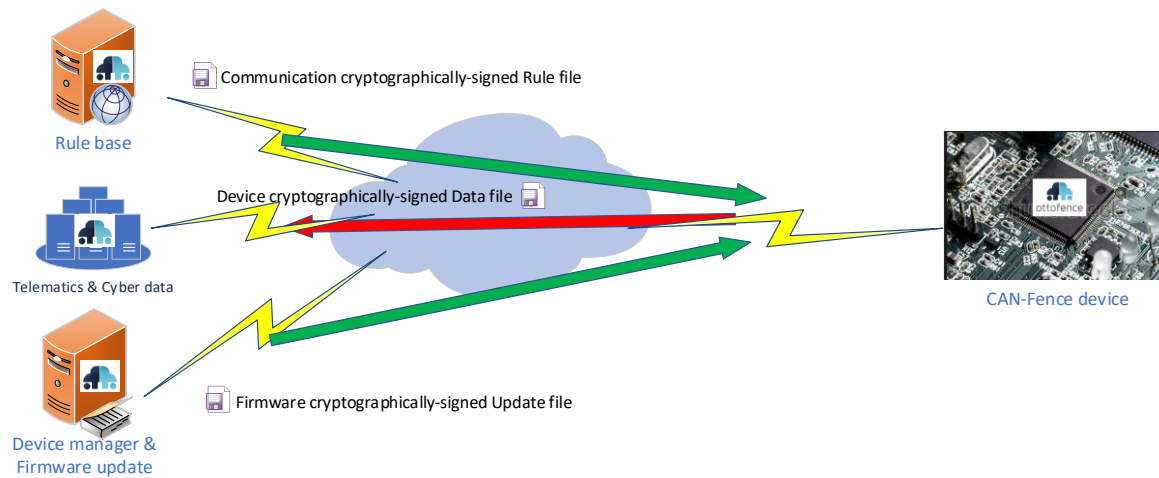
Enable services for customer

## Semi-Automatic 'Learning-mode' / Rule generation:

When a CANFence unit is installed in a new 'Installation-Type', the following process would take place:

1. The CANFence unit would be installed 'normally' between the vehicle CANBUS & Device
2. The CANFence unit would be placed in 'Learning' mode
3. Then, the vehicle would be driven normally for a pre-defined time (say few hours)
4. CANFence unit would generate a report file from the data it has collected, and upload it
5. Ottofence Server will process the file, and **automatically generate** an initial **Rule-Set**
6. The Rule-set is validated and will be stored in a **Ottofence database**, to be used with this Installation-Type in the future

# Secure data exchange





# Business Model

- **After Market**
  - Installation and ownership cost
  - Monthly Fee : Security Updates and Reports
  - Site / yearly license for Organizations
- **OEM**
  - Integration of HW & SW into OEM boxes
  - CANFence as System On a Module (SOM)
  - Monthly Fee

# The Team

- **Naftaly Sharir – CEO & CTO :**

Serial Entrepreneur; Technical & Business Leader and Manager : HW , SW & Systems  
30 years of Business & Technical experience in Communication, Internet, DSP, Audio, Video, VLSI, Cyber.

Reach career in **Multimedia Signal Processing , wireless, and mobile** began at **SIPL , IBM Haifa Research Labs**. Following as VP R&D at **VDOnet**, CEO at **Emblaze Semi**, CEO at **Electronics-Line 3000 Ltd**, CEO at **Advasense**.  
Co-founder at **Vitalitix**, Co-founder **Pixie-Technology**, CTO at **Terafence**

Holds a B.Sc. in EE (Cum Laude) from the Technion

Experience with setting up companies, Fund raising ( over \$40M at few companies ), Aggregated sales of about \$100M , few M&A process , coauthor of about 15 patents application

- **Adam Tal – R&D Manager:**

Over 20 years of experience in software and hardware development.

Experienced in Software **Architecture, Real Time, Electronics, IT, Network Architecture, Cyber Security and Automotive** product design.

Adam's Rich career in software engineering began at **Zoran**.

later worked for **Traffilog**, designing and implementing Telematics products for the Automotive market.

## Current Status, Accomplishments to date, AND use of Funds

- CANFence – CANBUS Firewall : HW and SW design- prototype is ready ; Design for secure connectivity ; Starting to work with professional penetration test ;
  - CANFi – CANBUS interface to WiFi : HW and SW design – available as an internal tool
  - OF CAN TOOL – CANBUS Analyzer : PC/Win tool. Analysis and Injection of CANBUS messages
- 
- CANFi – Consider as a product ... Enabled for use at the SIPL lab for Automotive Cyber Security project



CANFence

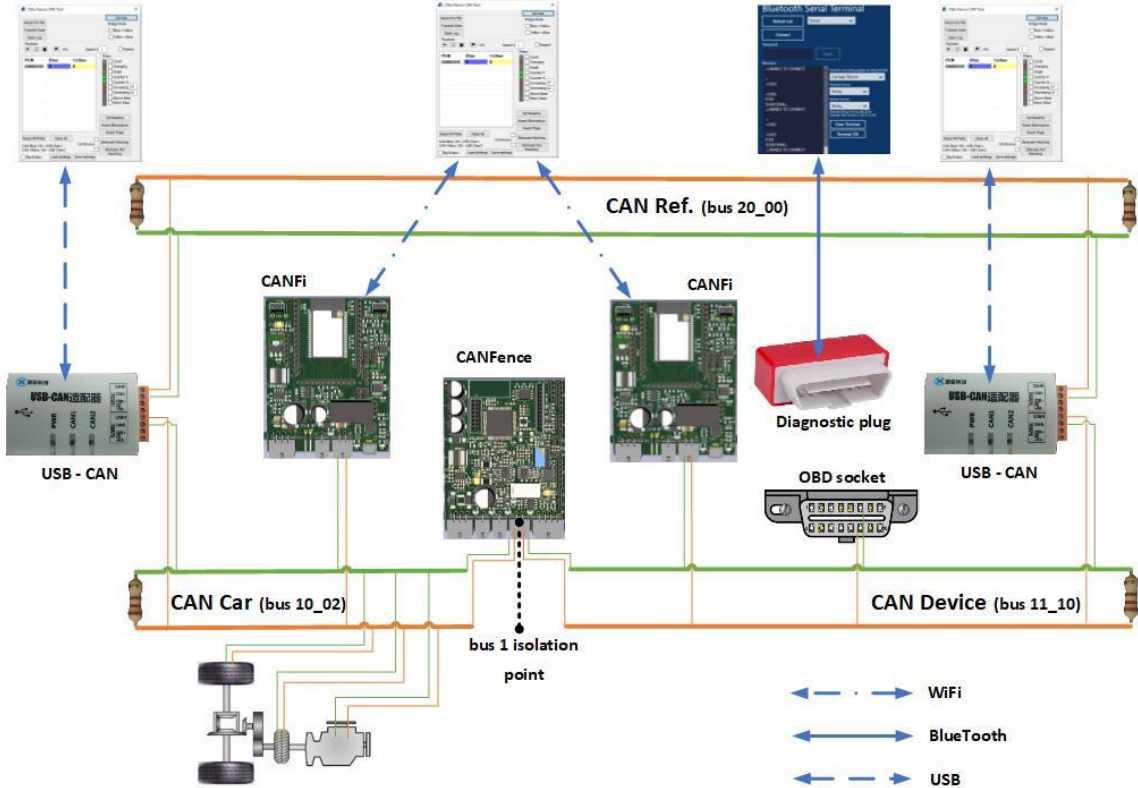


CANFi



OF CAN TOOL

# QA and Demo Setup



[Demo Video](#)

[QA and Demo 1](#)

[QA and Demo 2](#)

[QA and Demo 3](#)