Risk-based design for automotive networks

Eric Evenchik, Linklayer labs & Motivum.io
Stefano Zanero, Politecnico di Milano & Motivum.io

Who are we

Eric Evenchick

Linklayer Labs (Toronto, ON)

Eric has worked on OTA firmware updates and security design at Tesla Motors and Faraday Future. His experience in automotive began with research in alternative fuel vehicles at U. Waterloo, in conjunction with the US Environmental Protection Agency and General Motors. More recently, he founded Linklayer Labs, and released CANtact, an open-source hardware tool for CAN networks.

Stefano Zanero

Politecnico di Milano

Stefano is an associate professor at Politecnico di Milano, and has over 13 years of experience in the security field, from intrusion detection to threat intelligence, to penetration testing of industrial control systems. He has founded a security services company that delivers security assessment services worldwide.

Unfortunately...

22
SEP 2016

BRAZILIAN EMBASSY AND CONSULATE WORKERS STRIKE

BY Dean Orbell
uirements Changes
PERMALINK

Brazil Visa Processing Update:

Individual staff members of Brazil´s Foreign Ministry are currently on strike, including some officers of Brazilian Consulates and Embassy in the United States. At this time, most consulates are not experencing visa processing delays.

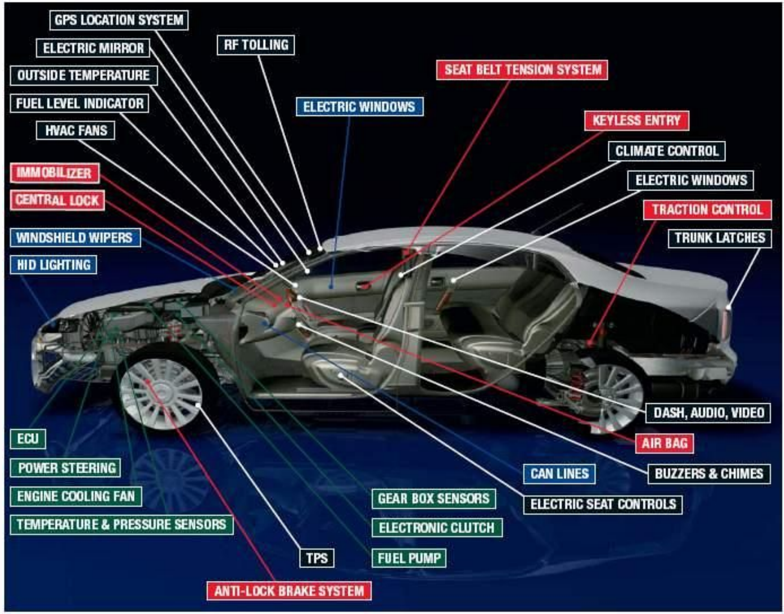
Automotive (in)security

Evolution of the Automotive World

Modern vehicle = hundreds of ECUs

Many connected systems

Varying levels of safety & security expectations



Attack example I

- Vehicle Theft

Attack example II

- Local Takeover

CarShark Software Lets You Hack Into, Control And Kill Any Car

Matt Hardigree
5/14/10 1:00pm · Filed to: CAR TECH

53.1K 185

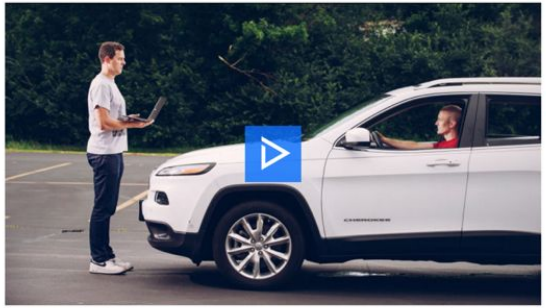
CarShark's a computer program that'll let someone hack into a car's onboard computer system to kill the brakes, disable the engine, blast music and otherwise wreak electronic havoc. It's both clever and absolutely frightening.

Attack example III

- Remote Takeover

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY —WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Hackers can easily drain the battery on the world's most popular electric car

Paul Szoldra
Feb. 24, 2016, 3:42 PM 1,836

FACEBOOK LINKEDIN TWITTER

The popular Nissan Leaf electric car can be drained of its battery life using little more than its vehicle identification number (VIN).

The major security hole was found by researcher Troy Hunt, who figured out that the Leaf's smartphone app interface (API) uses only the VIN to control car features remotely without passwords. These features include seeing the car's current battery life, times and distances the car has traveled, and

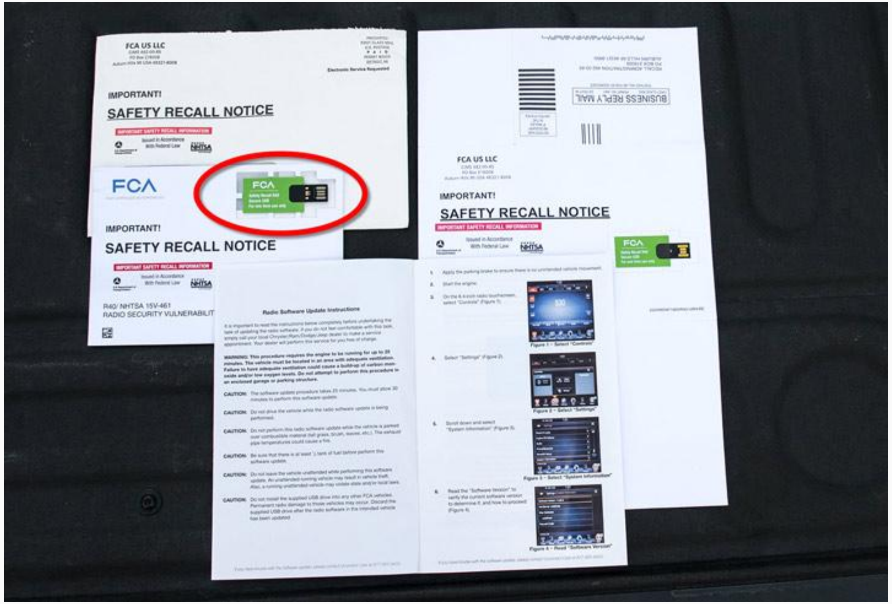
Attack Vectors

- Physical access to in-vehicle networks
  - Malicious mechanic
  - Aftermarket parts
  - Car sharing scenarios
  - Physical compromise
- Wireless protocols
  - Cellular
  - WiFi
  - Bluetooth
  - etc...

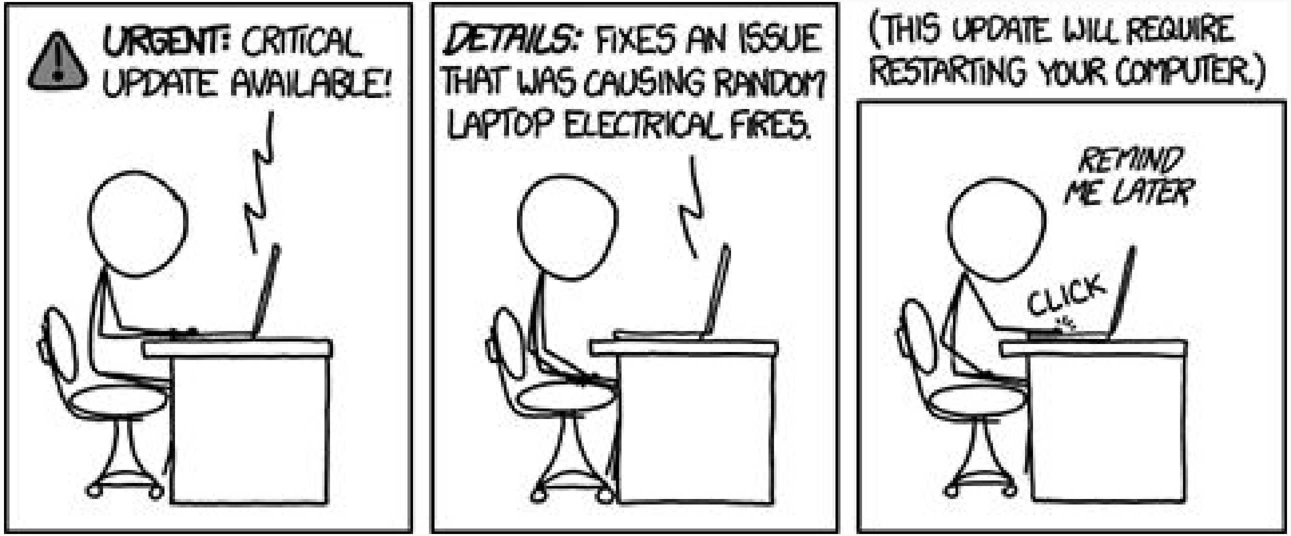
Attack Narrative is always similar

1. Attacker finds exploit in physical or wireless systems
   - Most of these systems not designed to be secure gateways
   - Changed assumptions, e.g. “if inside the vehicle, authorized”
2. Exploit is used to gain access to the in-vehicle network
   - Which was not designed to host non-trusted entities, so
3. Message forgery or diagnostics actions can be leveraged
   - Vehicle theft
   - Temporary modification of vehicle operation
   - Permanent modification of vehicle
   - Extraction of personal information, tracking, etc.

Defensive reactions...



Defensive (non) reactions...



Welcome to the Internet of Toasters

Where we find out that Twitter can be DDoSed by an army of toasters with “admin:admin” as their toasting credentials

(credit: https://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/)

Mirai Botnet Linked to Dyn DNS DDoS Attacks

FP_Analyst | Published in October 21, 2016 | Cybercrime, Emerging Threats, Trending | 284 views

SHARE IT

Key Takeaways

- Flashpoint has confirmed that some of the infrastructure responsible for the distributed denial-of-service (DDoS) attacks against Dyn DNS were botnets compromised by Mirai malware.
- Mirai botnets were previously used in DDoS attacks against the “Krebs On Security” blog and OVH.
- As of 1730 EST, the attacks against Dyn DNS are still ongoing. Flashpoint is coordinating with multiple vendors and law enforcement to track the infected devices that constitute the botnet being used to conduct these attacks.
- Flashpoint will continue to monitor the situation to ensure that clients are provided with timely threat intelligence data.

In summary:

- We cannot rely on **patching single vulnerabilities**
- Sound security engineering **does not start from vulnerabilities**
- Designing an **invulnerable** system **is not and can not be** the point
- **Risk = AssetValue x AttackVectors x Threats**
- We need to conceptually address the **risk** while **designing the networks**

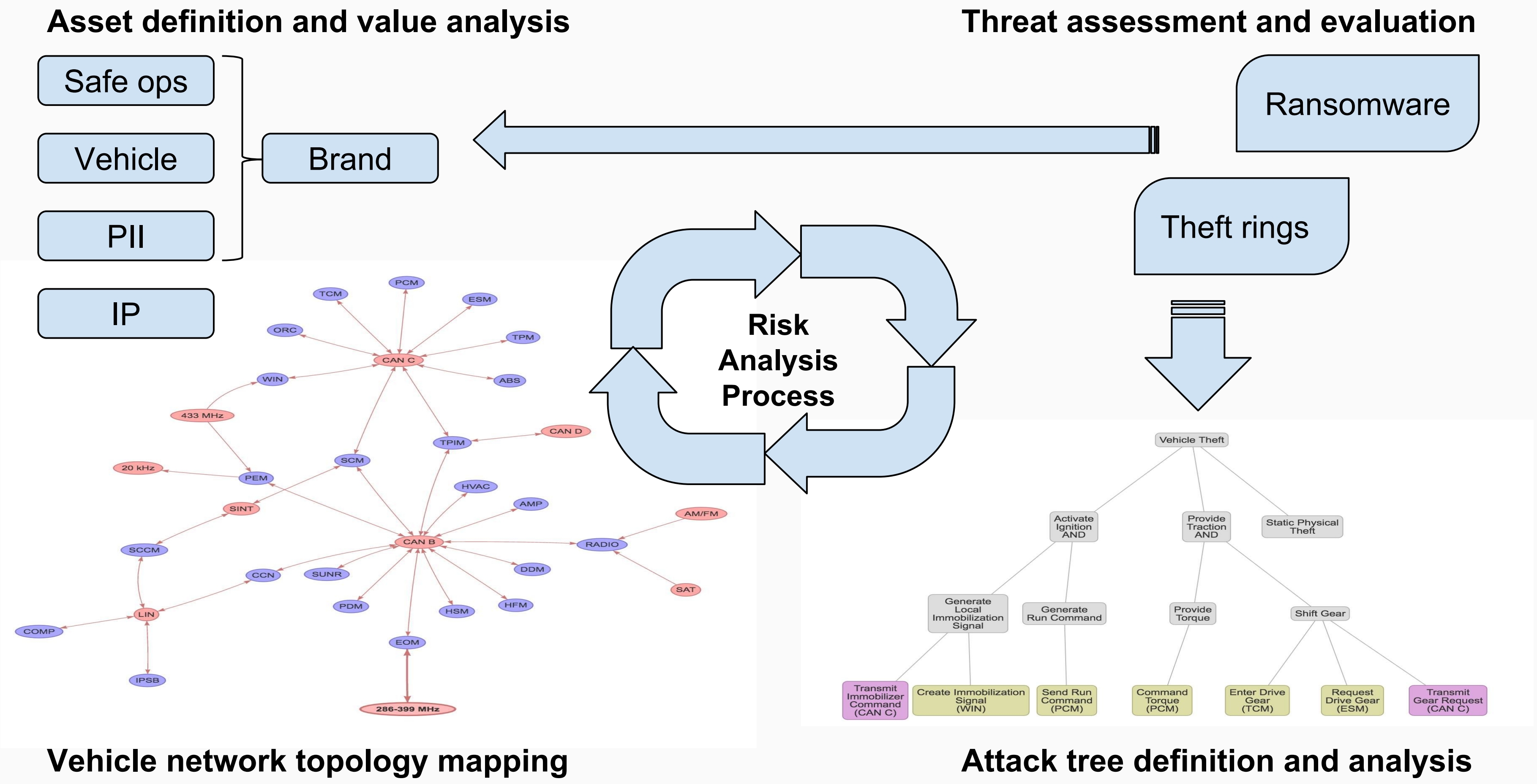
Our proposed approach

How do we model risk?

- Sound security engineering moves from **risk analysis**
- How to model risk in automotive scenarios?
  - The **risk assessment process** should be compliant with the standard set forth in SAE J3061 (more on this later)
  - Should be based on open standards and open access research (e.g. the EVITA model)
  - Should scale (from a whole vehicle to a single ECU)
  - Should be supportable with an **analysis tool** or generally be analytic enough to be computer-supported

Key intuition

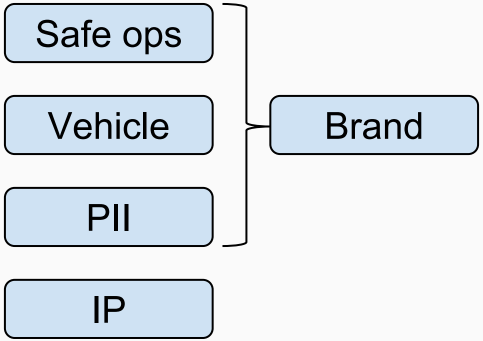
We want to **map risks** onto the **topology** of the vehicle network, and its **hardware and software components**



A complete methodology for risk assessment & secure network design

Step 1: asset definition

- Define the asset components for an appropriate risk evaluation
- Turns out that **this is quite simple** in automotive world
- Brand Impact, Compliance Risk, Insurance Risk, …, are all functions of the four asset categories listed
- Different players will have different risk definitions
    - E.g. OEM vs operator of a fleet of vehicles



Step 2: threat assessment

- Identify the main **threat agents**
- Evaluate **motives**
- Determine **likelihood** of attack scenarios
- Evaluate **goals**

Examples:

- Stunt hacking researchers :-)
- Theft rings
- Tuners
- Ransomware
- Competitors
- Targeted attacks
- Terrorism/State-sponsored/Military cyber-adversaries
- ...

Ranking exercise

- How would you rank the threats on the right by **likelihood**, based on public information right now?

- Stunt hacking researchers :-)
- Theft rings
- Tuners
- Ransomware
- Competitors
- Targeted attacks
- Terrorism/State-sponsored/Military cyber-adversaries

A (plausible) ranking

1. **Theft** ← By far the most likely

2. Tuners
3. Competitors
4. Hackers/Researchers

← YMMV with these

5. Cybercrime (ransomware)
6. Targeted attacks

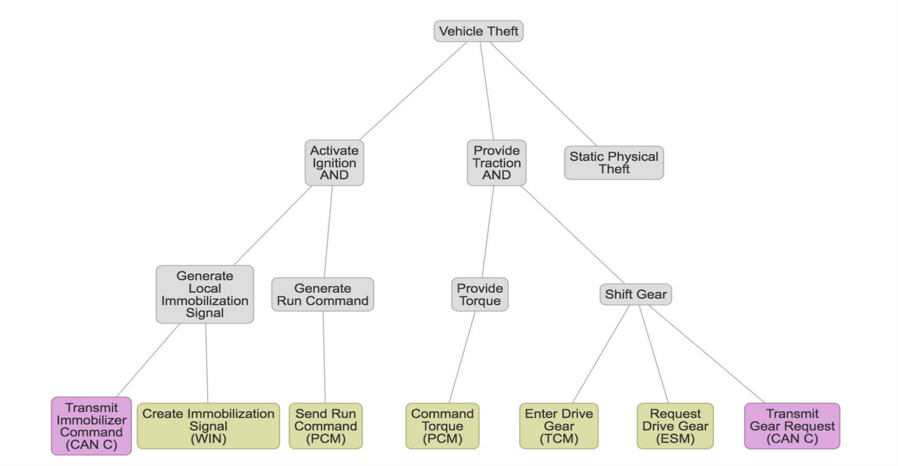
← Prediction: likely to grow

Example: theft

- Very good and reliable statistics to determine **likelihood**
- Impact: basically **vehicle** value (with secondary impact on brand, insurance costs…)
- What are the goals of a cyberattack brought by a theft ring? Basically **stealing** a vehicle

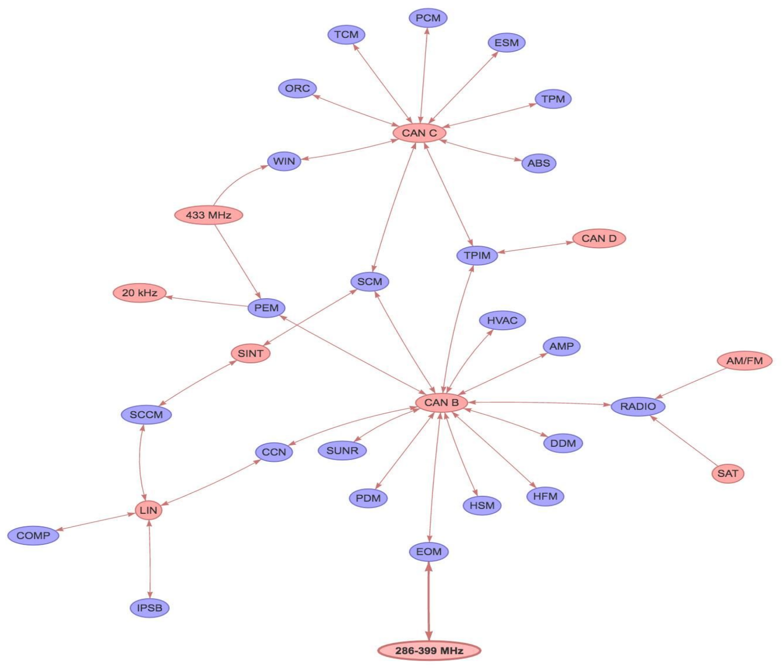
Step 3: attack tree breakdown

- For each identified **attack goal** we can use a generalized attack tree to break it down into attack scenarios
- We can then specialize this attack tree by connecting it to specific functionalities of the ECUs within the network

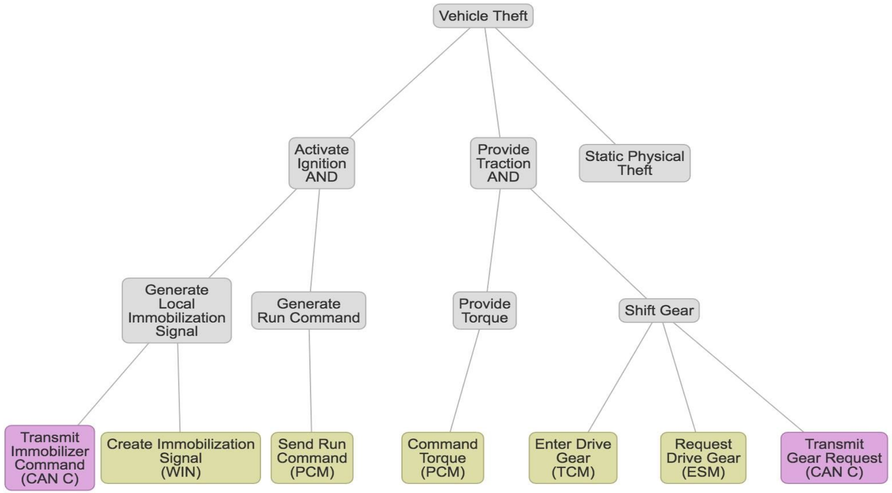


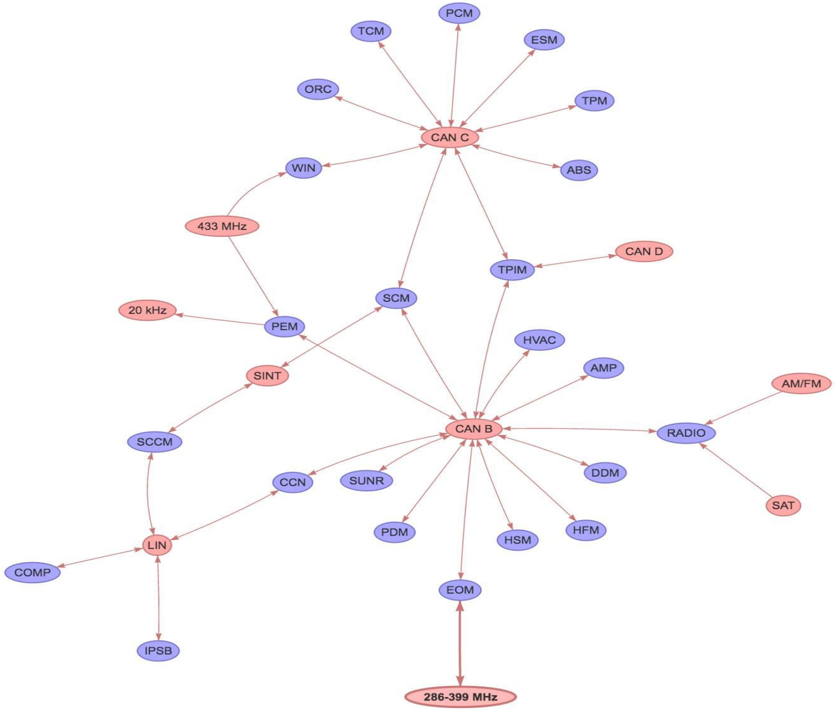
Step 4: network mapping of vehicle

- We can connect the **attack goals** to **specific vehicle components**
- This allows the designers to:
  - **Prioritize** analysis efforts to ECUs that are on important attack paths
  - **Generate** a set of tests/security specifications according to which we will test the ECUs
  - Propose **applicable solutions** according to a sensible risk reduction/treatment approach

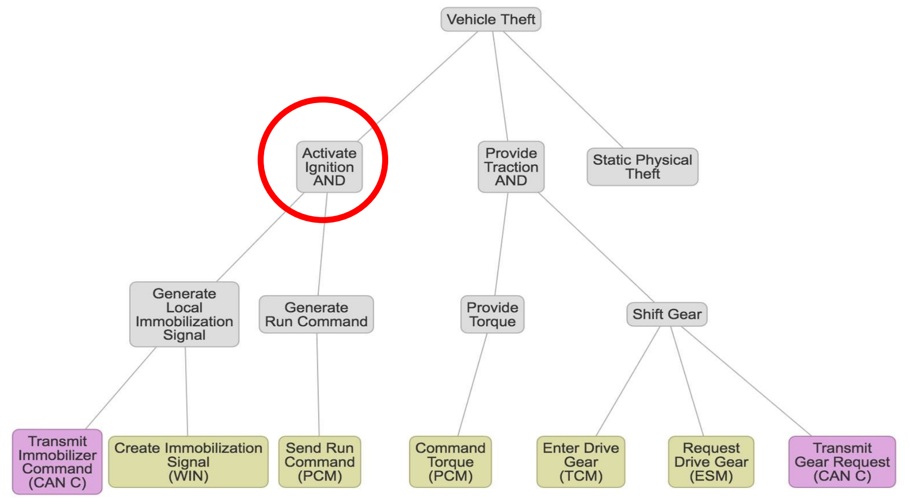


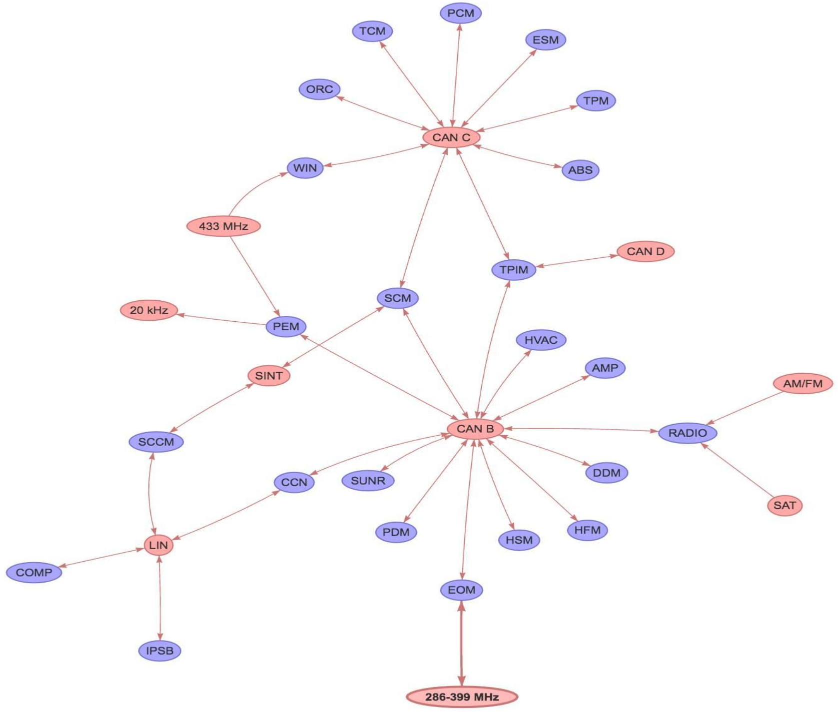
Mapping potential attacks onto the topology



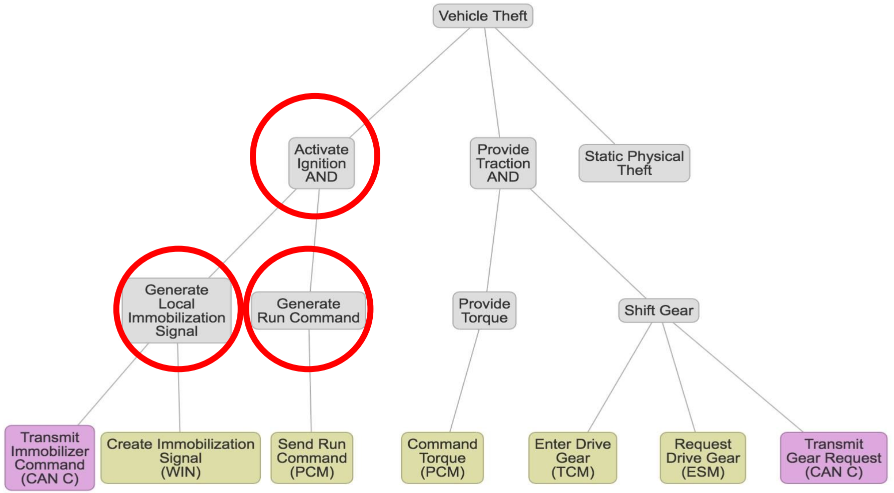


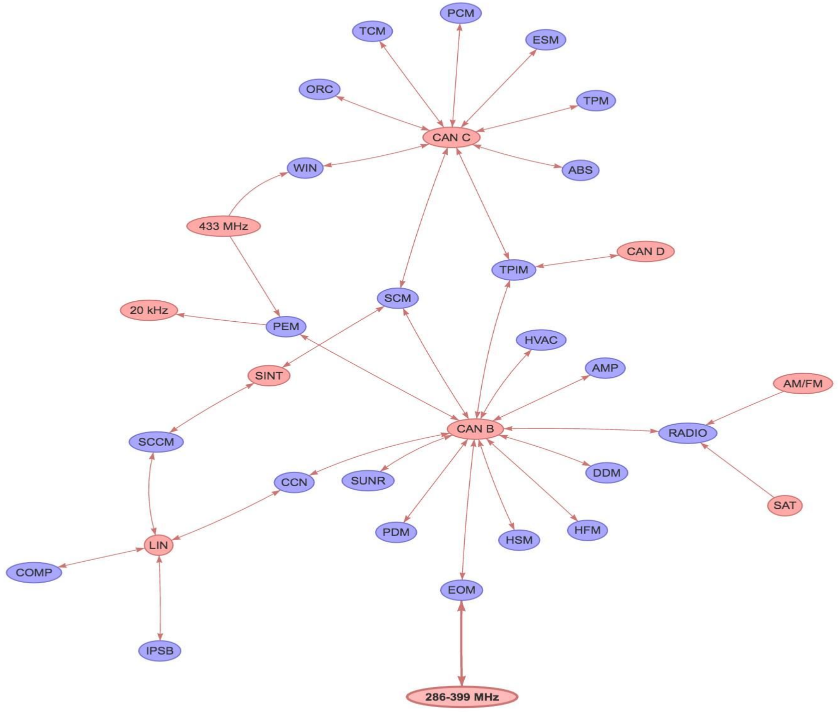
Mapping potential attacks onto the topology



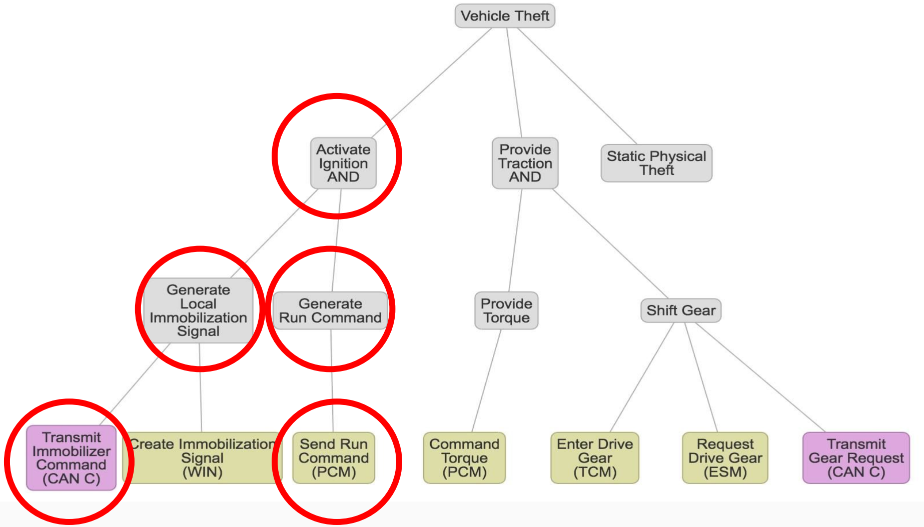


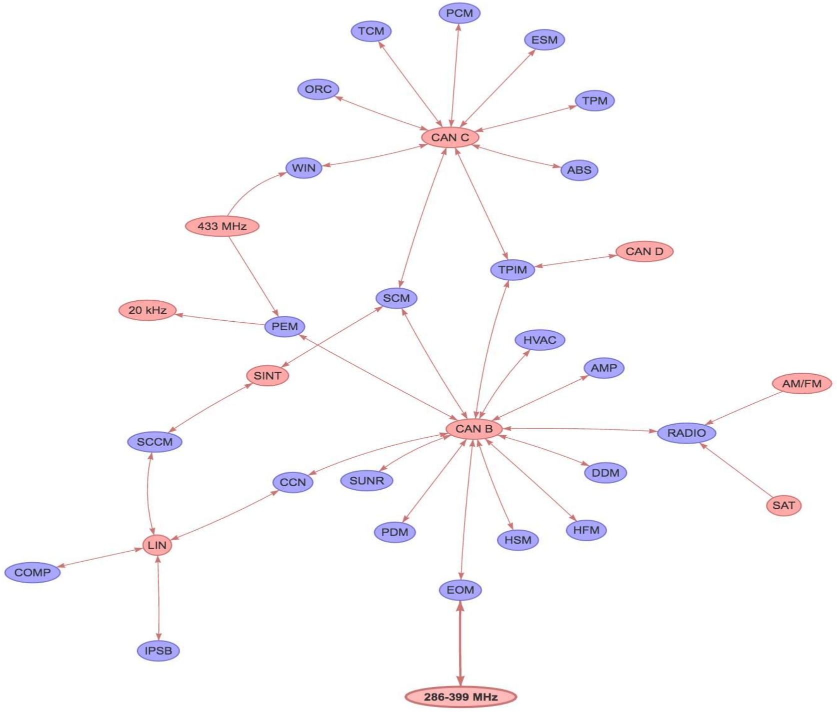
Mapping potential attacks onto the topology



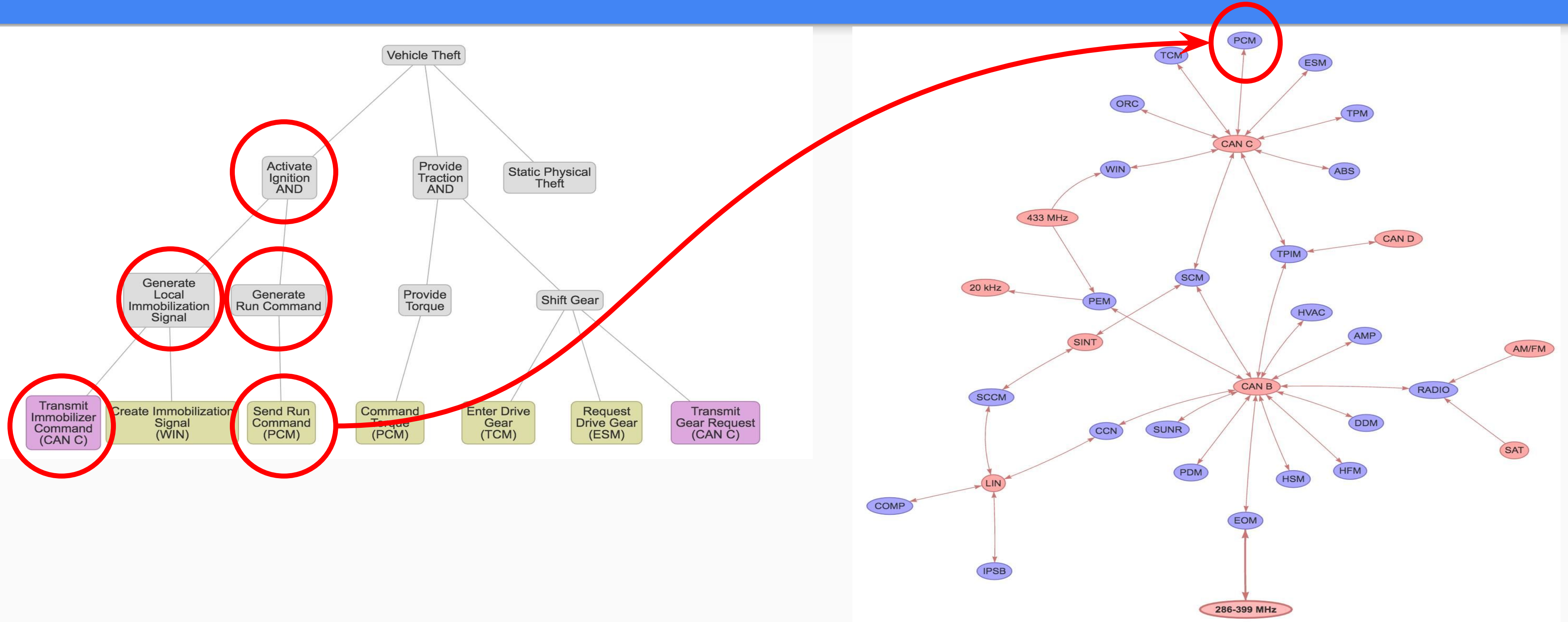


Mapping potential attacks onto the topology

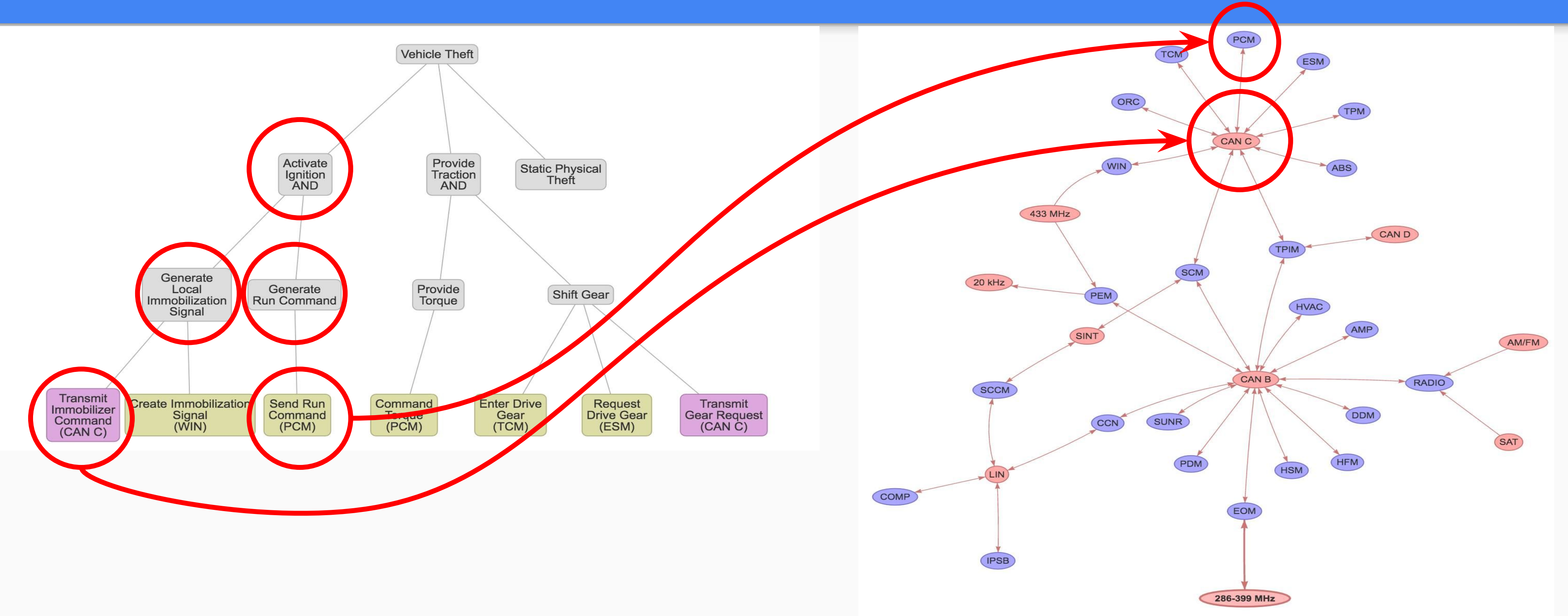




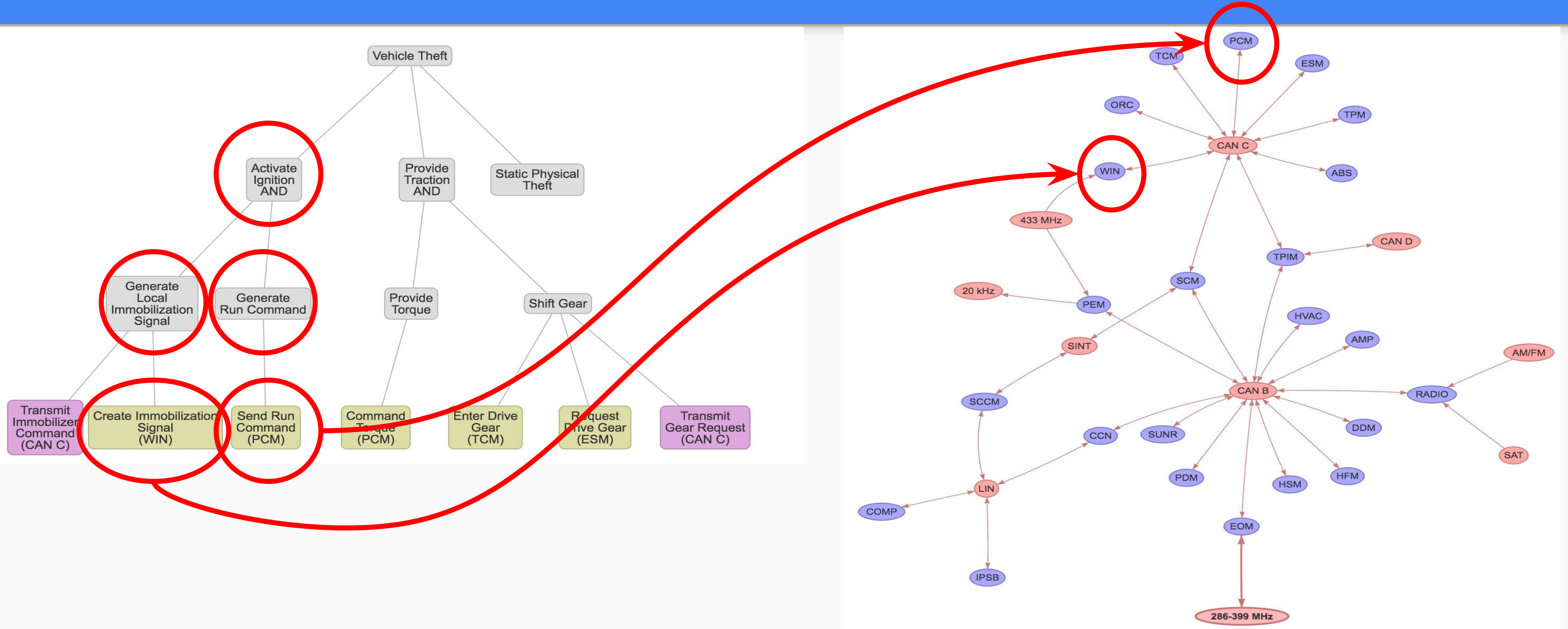
Mapping potential attacks onto the topology



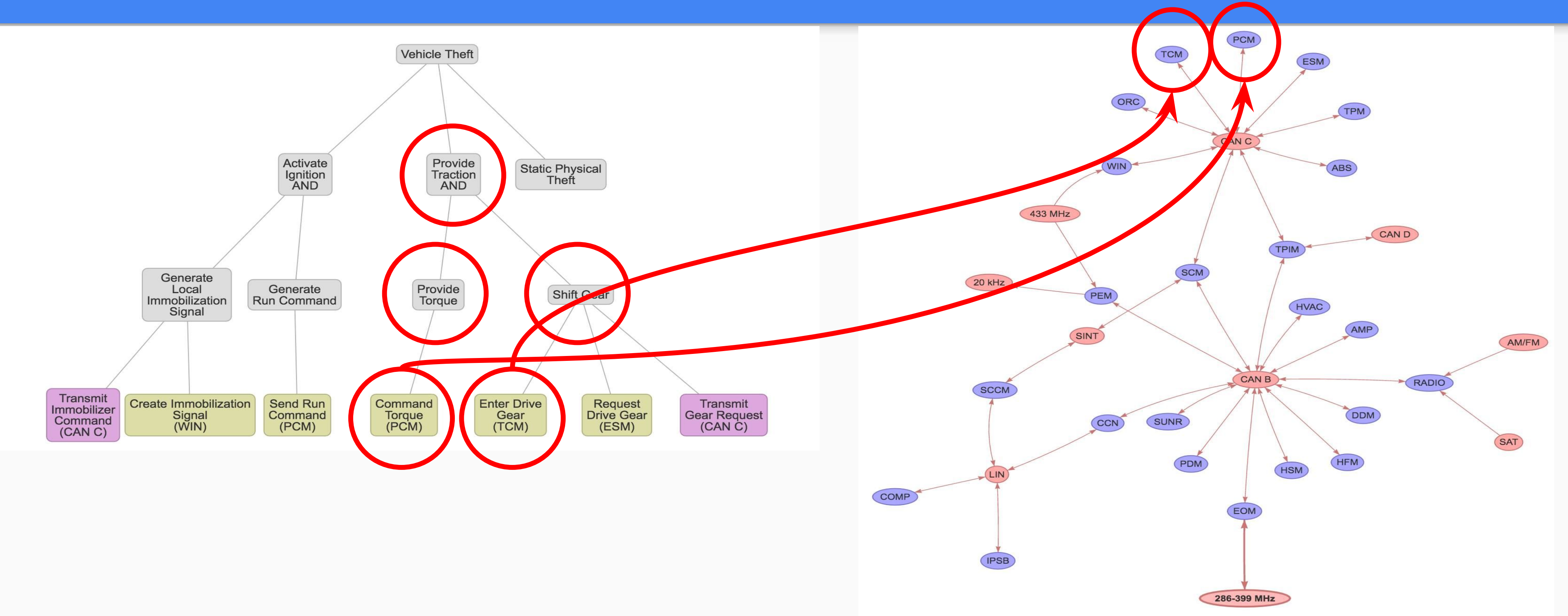
Mapping potential attacks onto the topology



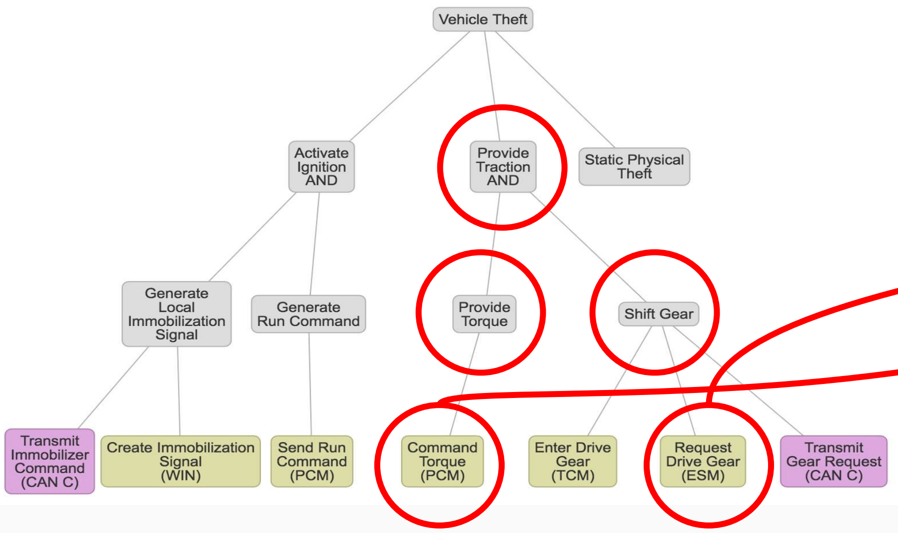
Mapping potential attacks onto the topology

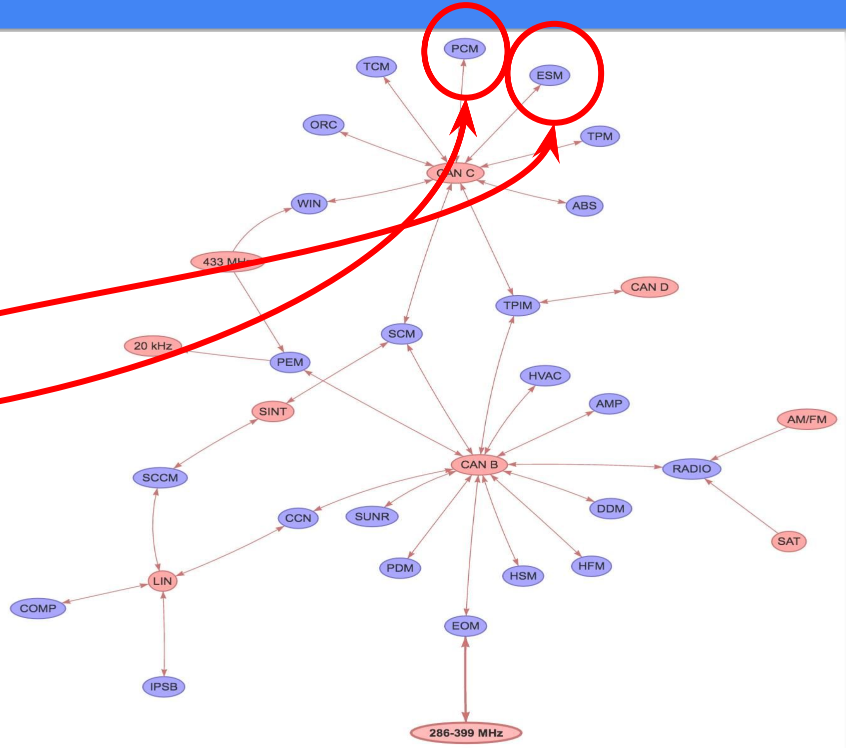


Mapping potential attacks onto the topology

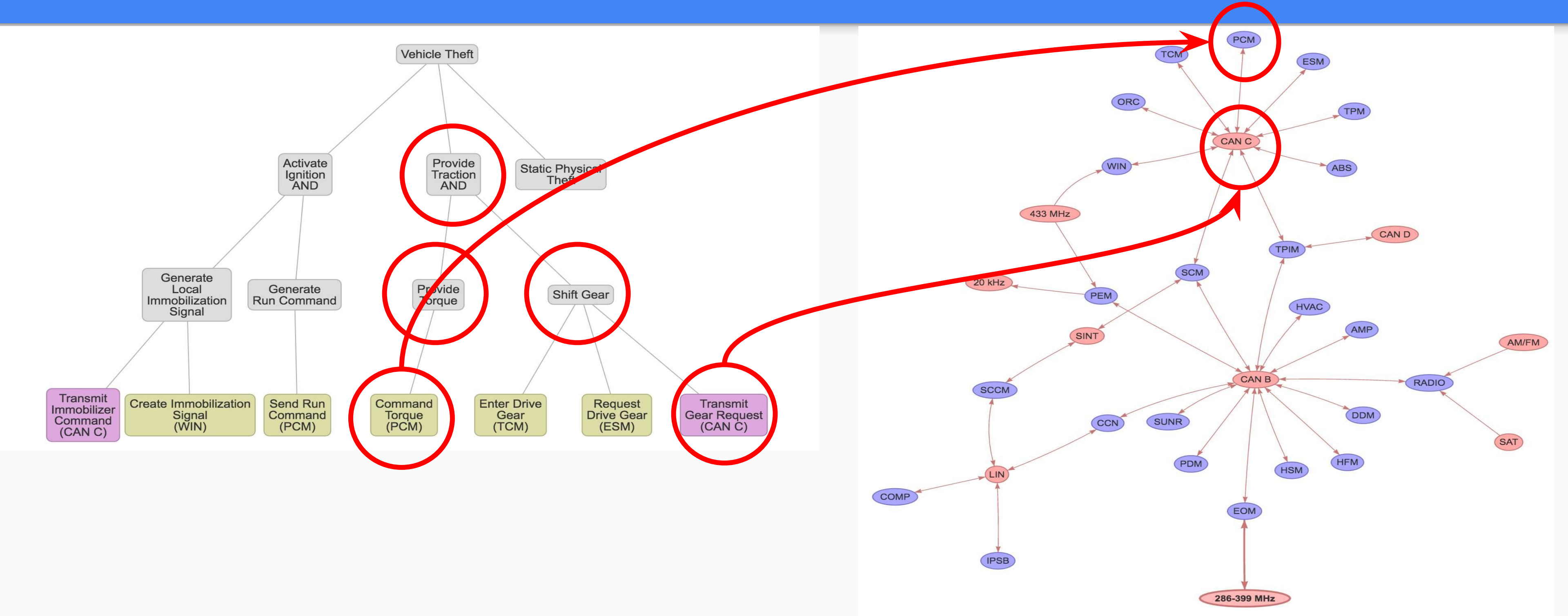


Mapping potential attacks onto the topology

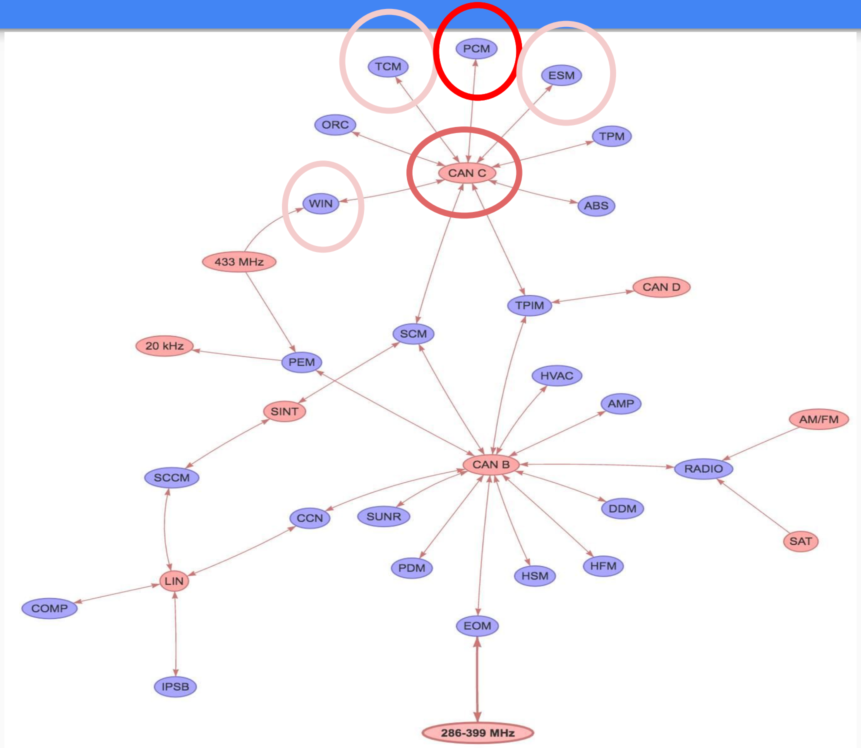




Mapping potential attacks onto the topology



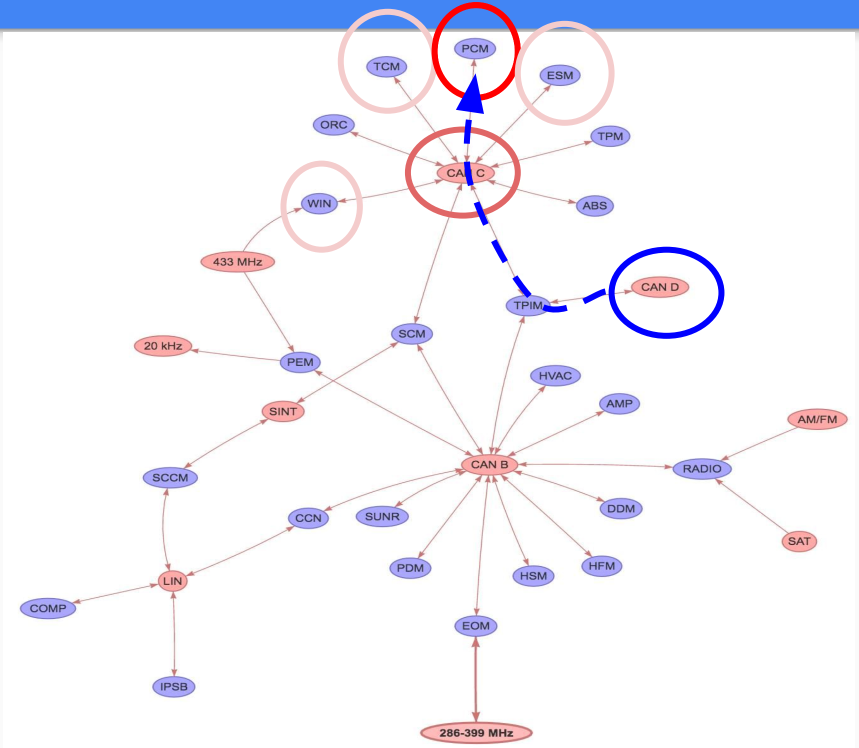
Attack vectors and ingress points analysis



Attack vectors and ingress points analysis

We now can use the identified attack vectors to:

1. Define security specs for, e.g., the TIPM module
2. Define ID rules (if any type of detection system is applied to CAN C)
3. Specify goals for penetration testing of each single component before acceptance



Responding to a pressing need...

SAE INTERNATIONAL

SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued 2016-01	
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems		

RATIONALE

To provide a cybersecurity process framework and guidance to help organizations identify and assess cybersecurity threats and design cybersecurity into cyber-physical vehicle systems throughout the entire development lifecycle process.

- Defines a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning.
- Provides high-level guiding principles.
- Provides information on existing tools and methods.
- Provides the foundation for further standards development.

TABLE OF CONTENTS

Our results easily map to EVITA (as an example)

Table 2 - EVITA severity classes

Class	Safety	Privacy	Financial	Operational
S0	No injuries	No unauthorized access to data	No financial loss	No impact on operational performance
S1	Light or moderate injuries	Anonymous data only (no specific driver of vehicle data)	Low-level loss (~$10)	Impact not discernible to driver
S2	Severe injuries (survival probable) Light or moderate injuries for multiple vehicles	Identification of vehicle or driver Anonymous data for multiple vehicles	Moderate loss (~$100) Low losses for multiple vehicles	Driver aware of performance degradation Indiscernible impacts for multiple vehicles
S3	Life threatening (survival uncertain) or fatal injuries Severe injuries for multiple vehicles	Driver or vehicle tracking Identification of driver or vehicle, for multiple vehicles	Heavy loss (~$1000) Moderate losses for multiple vehicles	Significant impact on performance Noticeable impact for multiple vehicle
S4	Life threatening or fatal injuries for multiple vehicles	Driver or vehicle tracking for multiple vehicles	Heavy losses for multiple vehicles	Significant impa multiple vehicle

Table 3 - Rating of attack potential and attack probability

Values	Attack potential required to identify and exploit attack scenario	Attack probability (reflecting relative likelihood of attack)
0-9	Basic	5
10-13	Enhanced-Basic	4
14-19	Moderate	3
20-24	High	2
>=25	Beyond High	1

In conclusion

- Security **cannot be bolted on** automotive networks one hack and one patch at a time
- We must embed **risk based security design** in the process
- We have devised a **simplified method**, and we are putting together a **supporting tool** to automate (most of) it
- This **implements the recommendations** of **SAE J3061**
- Want early access to the tool? Let us know!

Thanks for your attention!

Questions and feedback:

@raistolo
stefano@motivum.io

@ericevenchick
eric@motivum.io