Candy Cream

Gianpiero Costantino
Ilaria Matteucci
Vehicles are Cyber-Physical System
Attack Surface

Locale Vs Remota
Attack on Jeep Cherokee

C. Miller and C. Valasek, BlackHat 2015
Candy Cream

hacking infoAiNment AnDroid sYstems to Command instRument clustEr via cAn data fraMe
Attack Workflow

CANDY
- Android IVI exploitation through misconfiguration
- In-vehicle CAN bus network exploitation through the Android IVI

CREAM is the post-exploitation phase to inject forged CAN data frames
Android IVI Vulnerability Assessment

- **Recon** checks out the target using multiple sources
- **Scanning** maps out and investigates the network
- **Exploitation** attacks holes found during the scanning process
- **Elevation of Privileges** elevates a lower access account to root, or system level
- **Maintaining Access** uses techniques like backdoors to keep access to the target device
- **Covering their Tracks** erase logs, and manipulating files to hide the intrusion
Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. The ADB command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device.
In-vehicle network

Vehicles functionalities are managed by Electronic Control Units (ECU)

ECU communicate via CAN bus protocols
The CAN bus as is

Integrity ✗  Confidentiality ✗  Authentication ✗
Candy Cream - Demo
on a real vehicle
Thank you!

Find us on

https://sowhat.iit.cnr.it
WE WANT YOU!