
ARGUS
CYBER SECURITY

# Argus Cyber Security

Daniel Rezvani, Cyber Security Researcher

## Hacking Automotive Ethernet Cameras

October 2018

Email: Daniel.rezvani@argus-sec.com

# Argus - A Global Leader in Automotive Cyber Security

## HOLISTIC, MULTI-LAYERED PORTFOLIO

**5** Multi-Layered Solution Suites
Software Updates Over-the-Air
**51** Granted & Pending Patents
Trusted Advisory Services

## ONE STOP SHOP

PREVENT UNDERSTAND RESPOND

1st in 3rd-Party Evaluations!

## AUTOMOTIVE & CYBER EXCELLENCE

**Cyber:**

Decades of cyber security Expertise in embedded systems

**Automotive:**

Automotive cyber security veterans

## PARTNERING WITH INDUSTRY LEADERS

Continental The Future in Motion, EB, RENESAS, QUALCOMM, ST, MAGNA, NXP, intel Intel® INGENUITY PARTNER PROGRAM, Infineon, NVIDIA, ERICSSON, Check Point SOFTWARE TECHNOLOGIES LTD.

## WORKING WITH WORLD'S MAJOR OEMS & TIER 1s

**5** Offices Worldwide, **130** Employees

# Dozens of Penetration testing Projects,

# 100% Success Rate

Research Case Studies:

**1**

↘ Remote attack of an OEM's **TCU**

↘ Argus discovered > **22** vulnerabilities

↘ 6 classified as **high-risk**

**2**

↘ Remote attack of an OEM's **head unit**

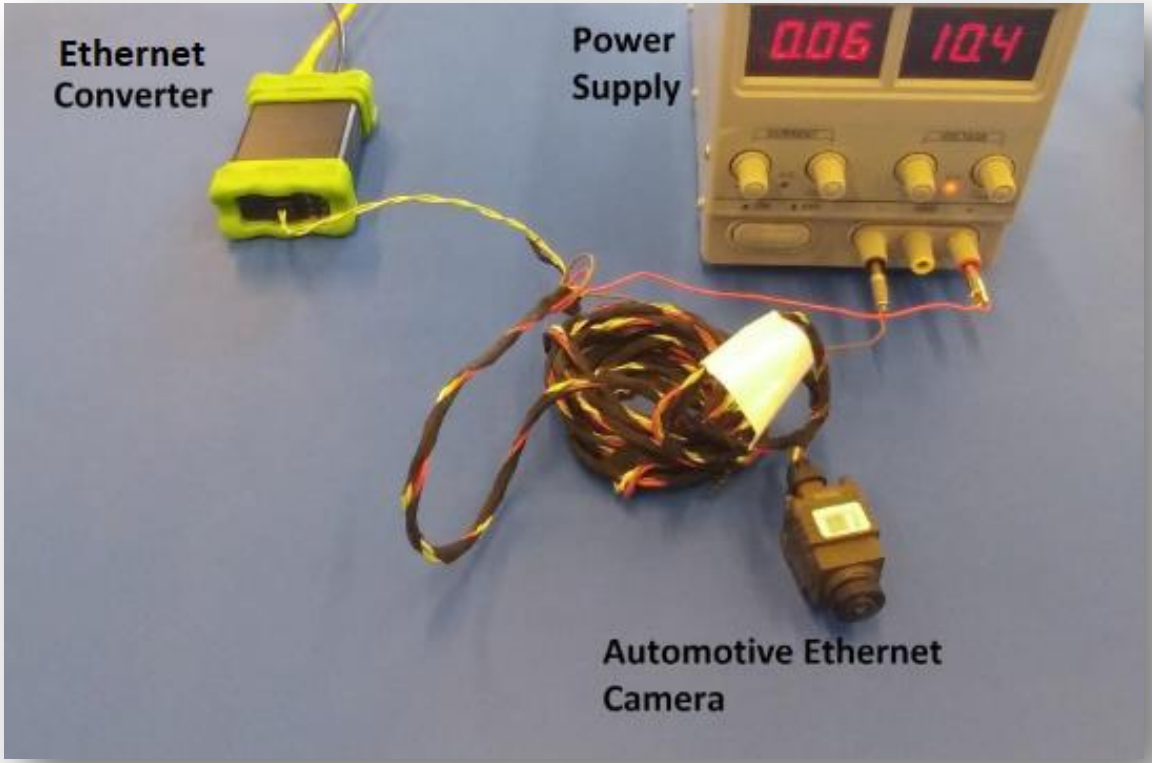
↘ Argus discovered > **25** vulnerabilities

↘ Most are **zero-days** vulnerabilities

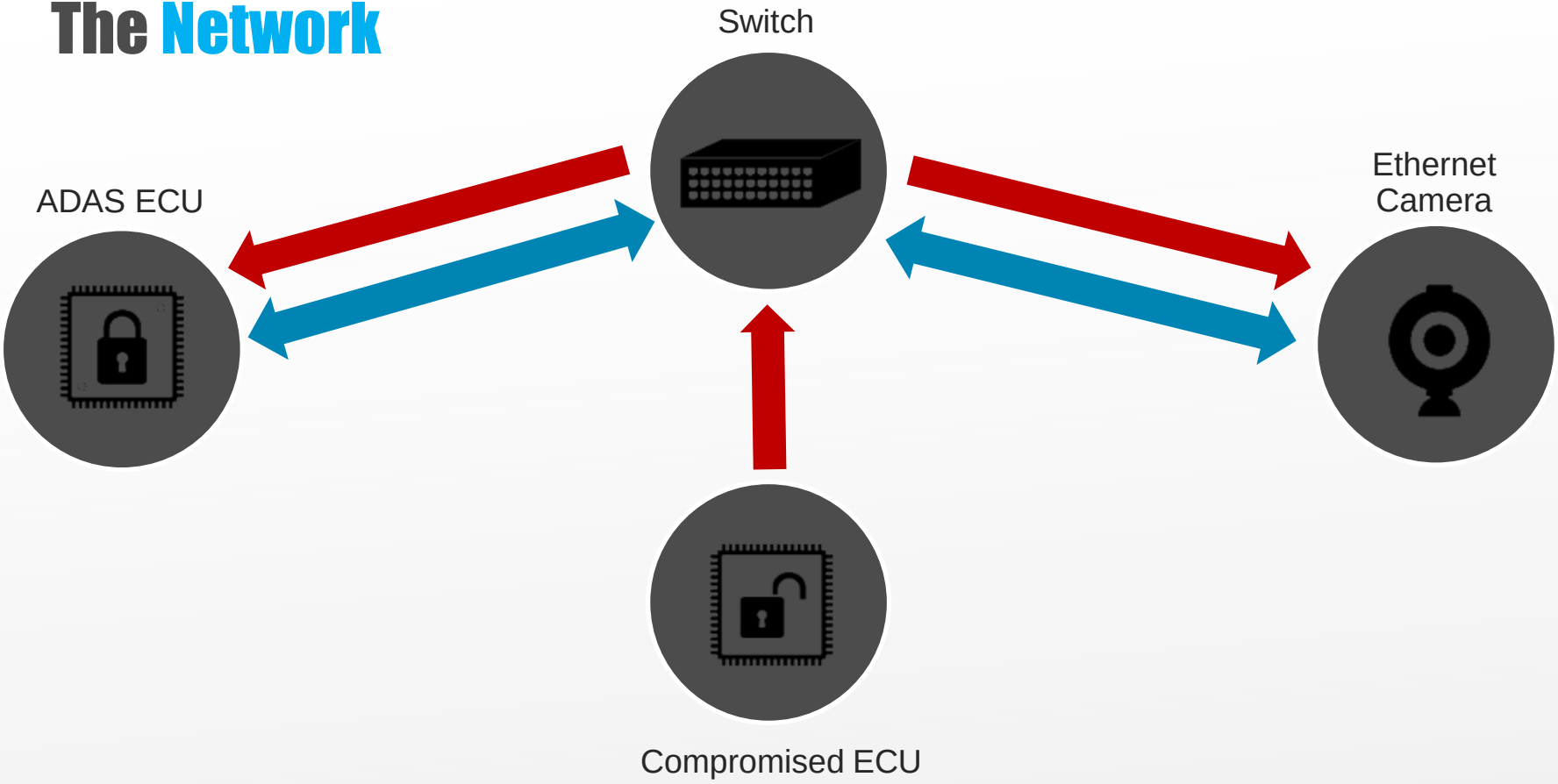
**Argus bypassed all security mechanisms and injected messages via SMS/Bluetooth into the in-vehicle network**

# Potentially Devastating Consequences

# The Setup


Ethernet
Converter
Power
Supply
0.06
10.4
Automotive Ethernet
Camera

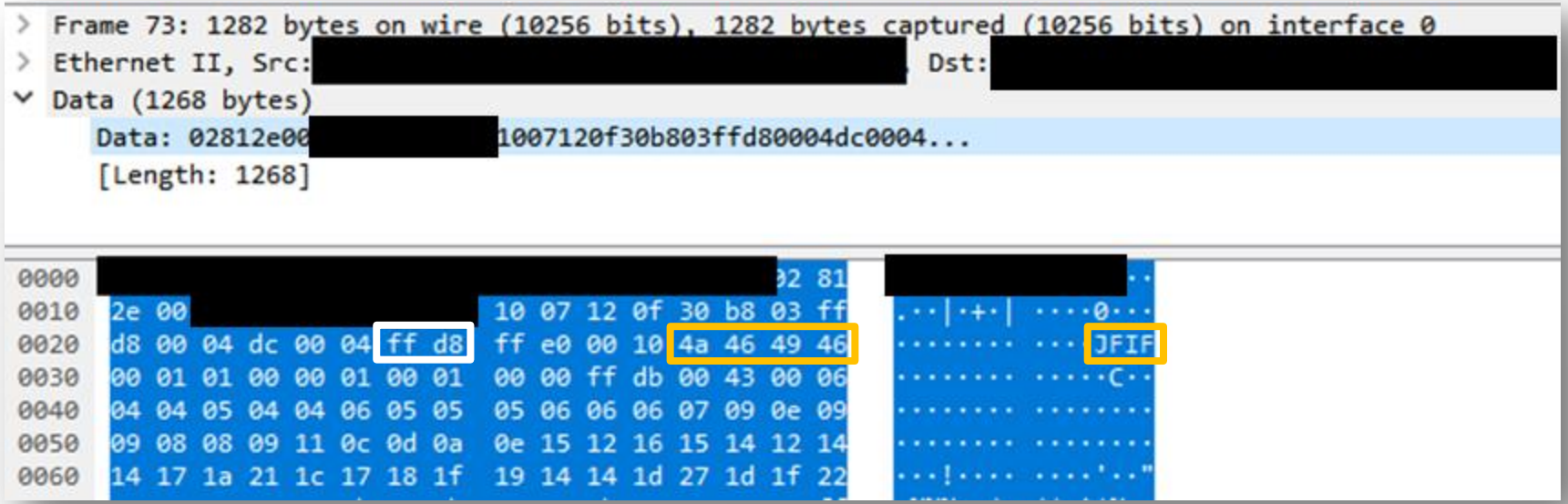
# The Network



# The Camera

- Lightweight DHCP on power up
  - Broadcast UDP packets until IP is received
  - Idle wait until command is received
- Command port
  - Only other open port
  - Receives UDP packets with command data
    - Start stream, stop stream, change FPS, etc.
- AVB Stream
  - JPEG payload
  - Approx. 2700 packets/second

# The Payload


Frame 73: 1282 bytes on wire (10256 bits), 1282 bytes captured (10256 bits) on interface 0
Ethernet II, Src: [redacted] Dst: [redacted]
Data (1268 bytes)
Data: 02812e00[redacted]1007120f30b803ffd80004dc0004...
[Length: 1268]
0000 [redacted]02 81
0010 2e 00 [redacted] 10 07 12 0f 30 b8 03 ff
0020 d8 00 04 dc 00 04 ff d8 ff e0 00 10 4a 46 49 46
0030 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 06
0040 04 04 05 04 04 06 05 05 05 06 06 06 07 09 0e 09
0050 09 08 08 09 11 0c 0d 0a 0e 15 12 16 15 14 12 14
0060 14 17 1a 21 1c 17 18 1f 19 14 14 1d 27 1d 1f 22
JFIF

# Denial of Service

# Denial of Service

- End of Image Attack
  - 2 data bytes per packet
  - Single packet every 10 ms
  - ~3.7% increase in overall traffic
  - ~0.0004% increase in overall data

- Additional Attacks
  - DHCP poisoning on power up
    - Race Condition
  - “Junk” stream
    - Large overhead (approx. 100% increase in traffic)
  - Stop stream command
    - Replicate the “stop” command
    - Idle camera – how can we take advantage of this situation?

# Stream Hijacking

# Stream Hijacking

- Pre-recorded “malicious” stream
  - After stopping camera, free to inject to client
  - Re-started camera after attack
    - Loop or stop instead
- Man In The Middle (MITM) alternative
  - Trigger
    - Legitimate start request from client injects malicious stream
  - “Latency Attack”
    - Delay packets between endpoints

# Research Summary

- No security mechanisms
  - Attacker can easily understand and replicate commands
  - Camera/client are unable to differentiate spoofed packets from real ones
- Proof of Concept
  - Different cameras and suppliers
  - Raise awareness
    - Cameras are not the center of attention for automotive cyber security
    - Potential danger


ARGUS
CYBER SECURITY

# CONTACT US

Daniel.rezvani@argus-sec.com