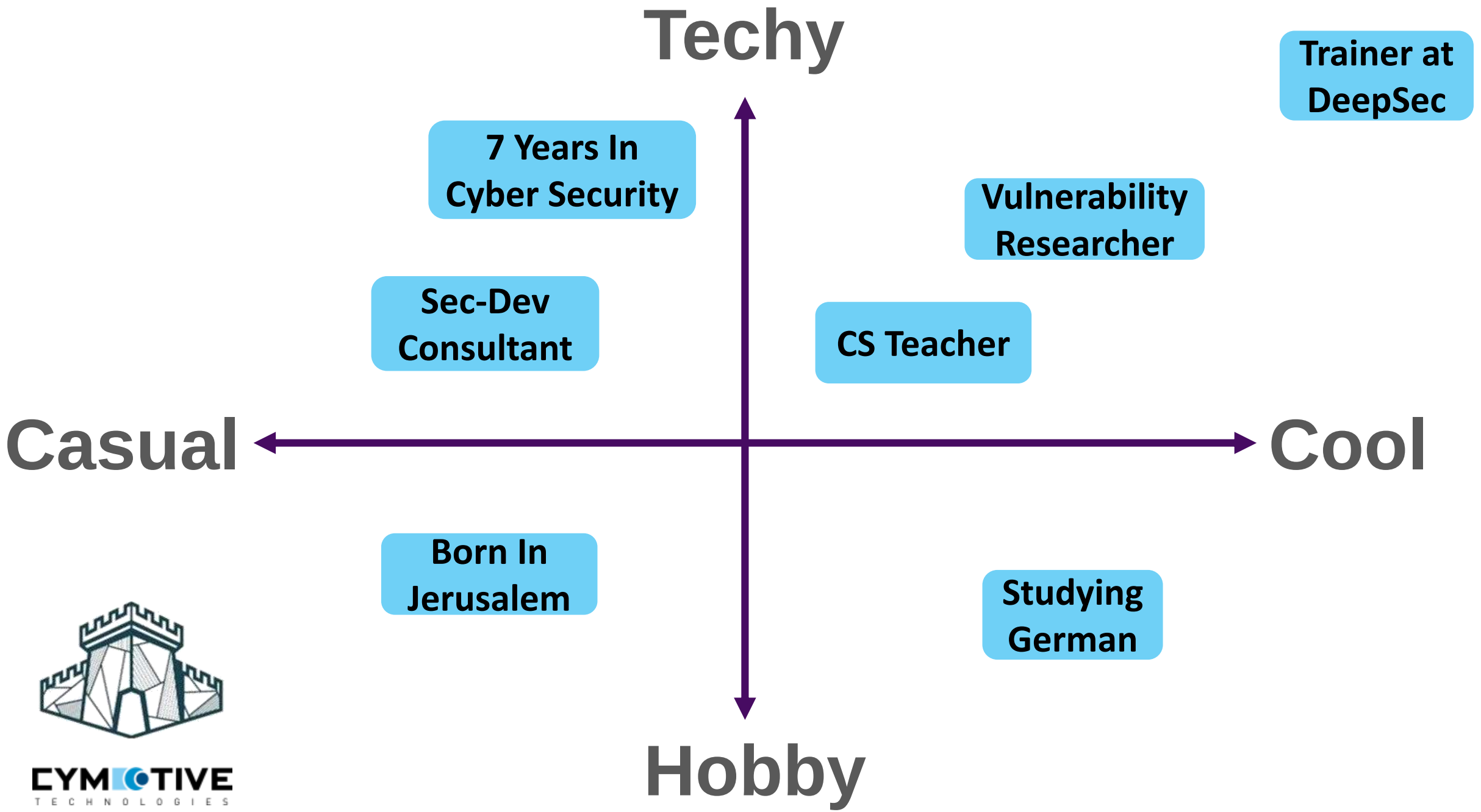
CYMOTIVE TECHNOLOGIES

The Future Is Here - Modern Attack Surface On Automotive

Lior Yaari

28/11/2019



CYMOTIVE TECHNOLOGIES

Imperium Security

TRAINING

Embedded Secure Development
Embedded Attack & Defense
Vulnerability Research and Exploits

WHITEBOX VULNERABILITY RESEARCH

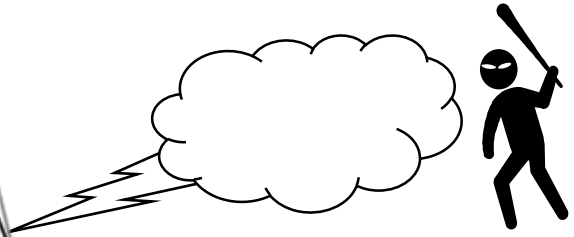
ARCHITECURE SECURITY

IMPERIUM SECURITY

CYMOTIVE TECHNOLOGIES

End to End Security Testing

Breaking through the cloud or factory



Bypassing ECU protections

Building Security Products

Vehicle Security Research

Disclaimer

As part of our job with CYMOTIVE we are working closely with several automotive companies and because of that many of our findings are under NDA.

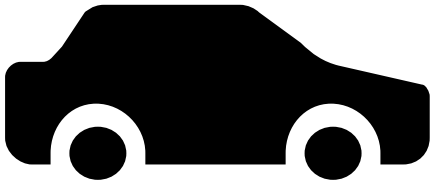
We will not include ANY customer names and real issues which can cause any harm and focus more on the tech side

**** All photos in this presentation are from open sources found on the internet***

CYMOTIVE TECHNOLOGIES

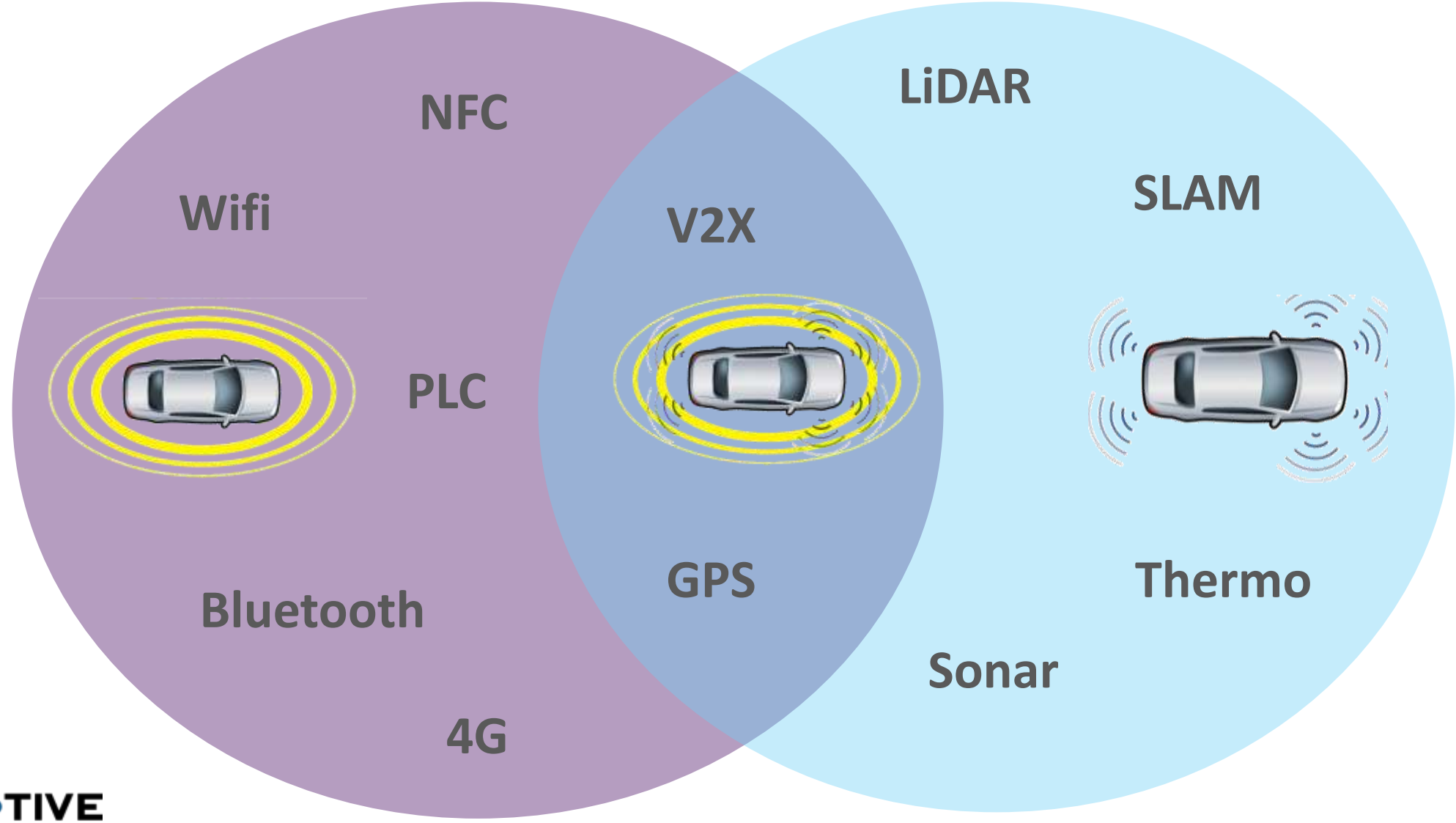
Progress Bar

- ~~Who I Am~~
- Automotive Past & Future
- Connected Technologies
- Centralized Management



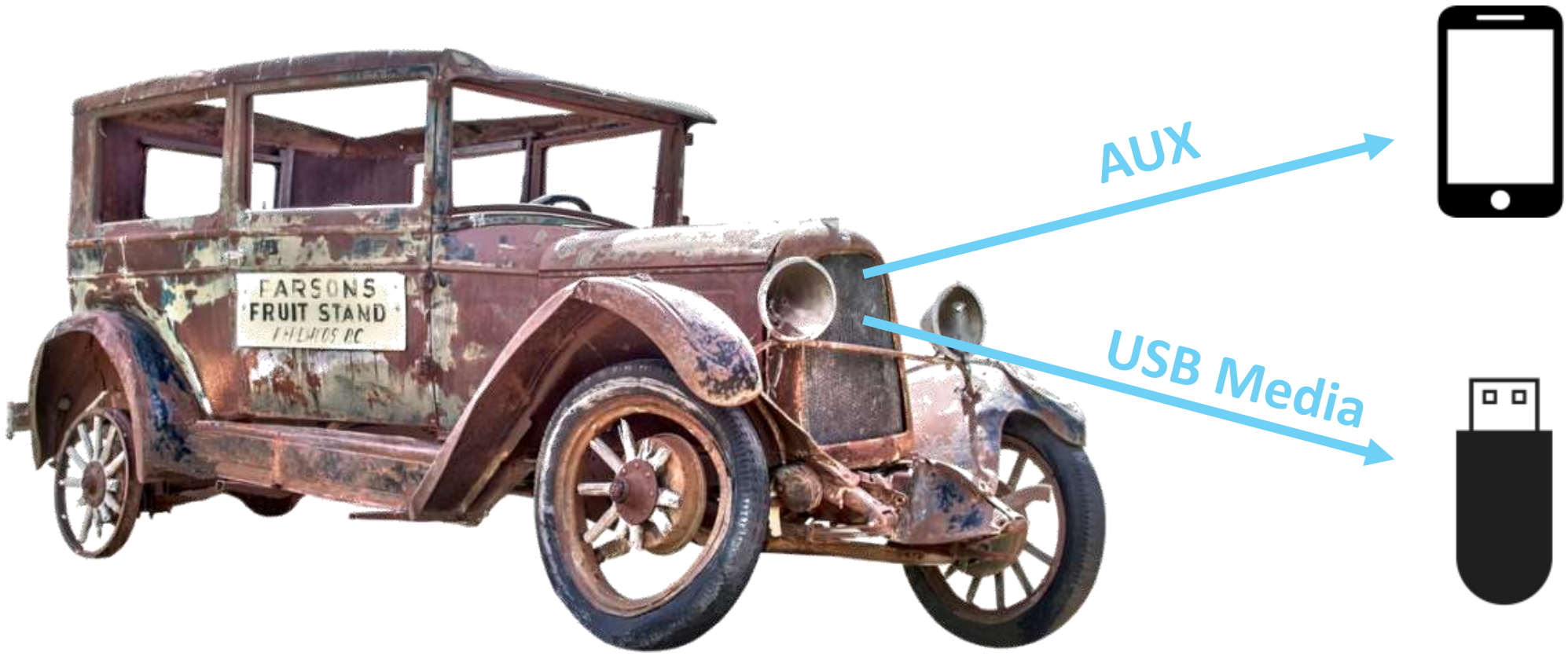
CYMOTIVE TECHNOLOGIES

Automotive Main Trends



CYMOTIVE TECHNOLOGIES

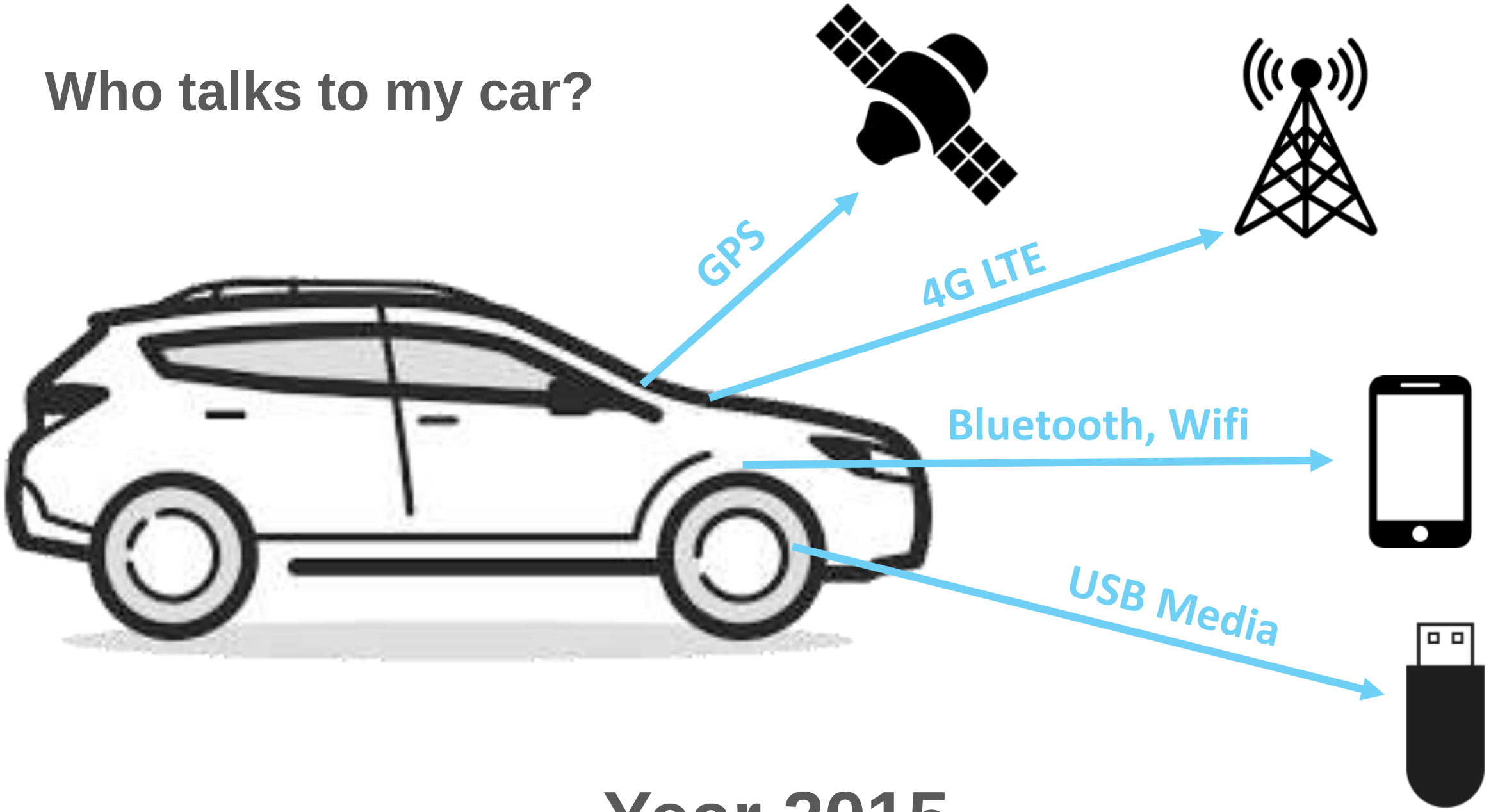
Who talks to my car?



Year 2005~

CYMOTIVE TECHNOLOGIES

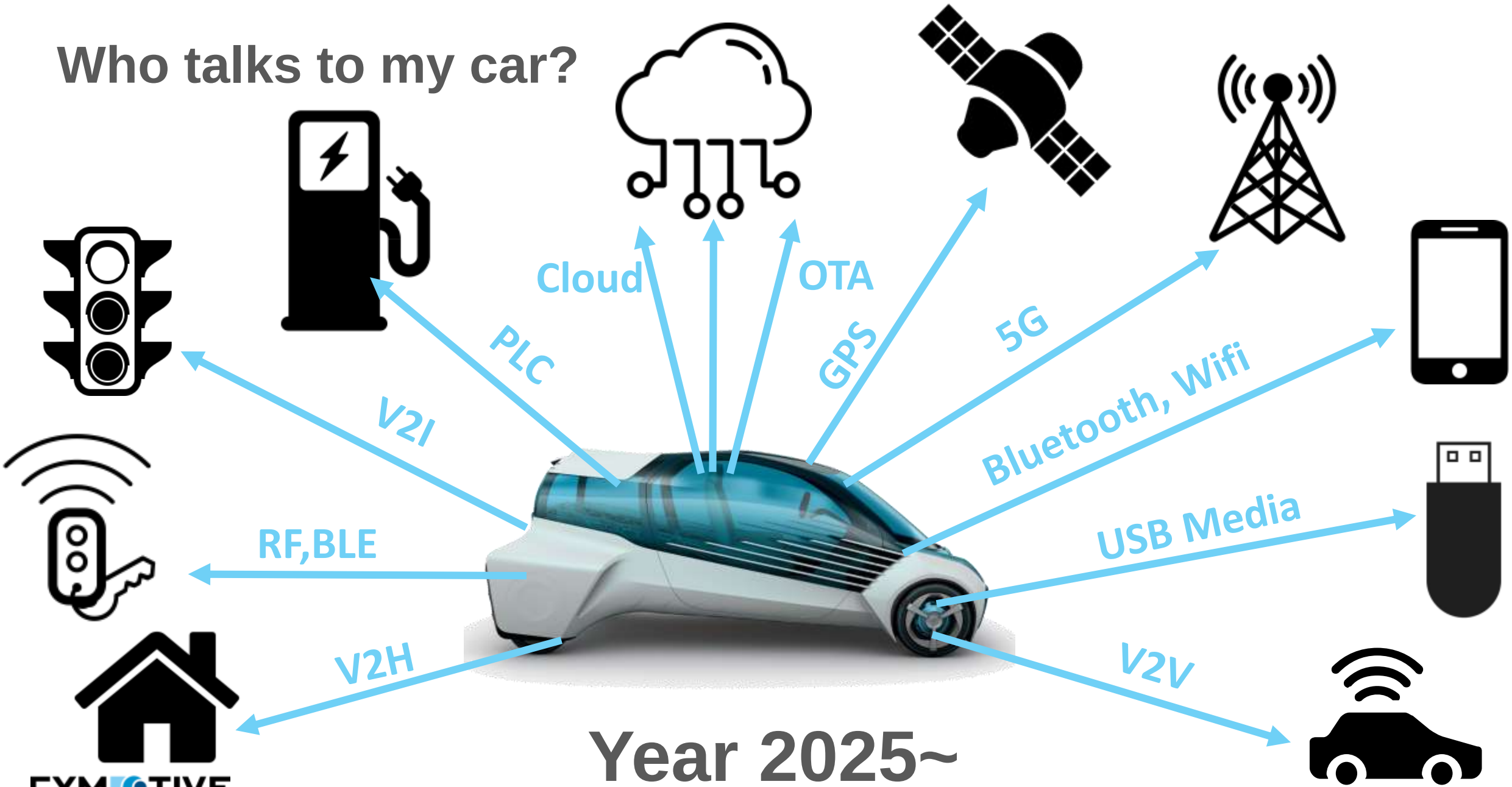
Who talks to my car?



Year 2015~

CYMOTIVE TECHNOLOGIES

Who talks to my car?



Year 2025~

CYMOTIVE TECHNOLOGIES

What does it imply?

Changes

CAN Bus

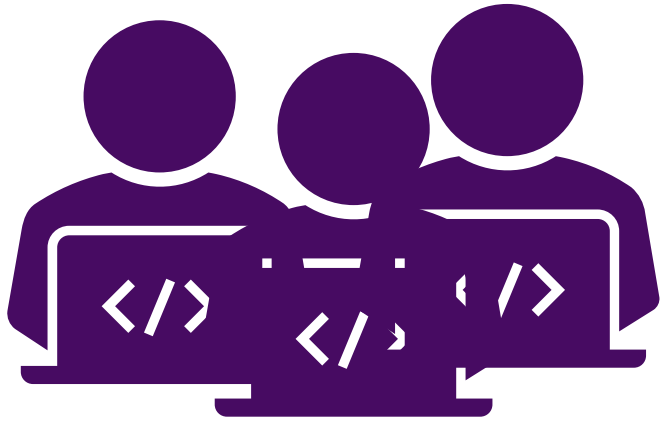
Mechanical Engineer

Ethernet

Software Developer

CYMOTIVE TECHNOLOGIES

New Demands



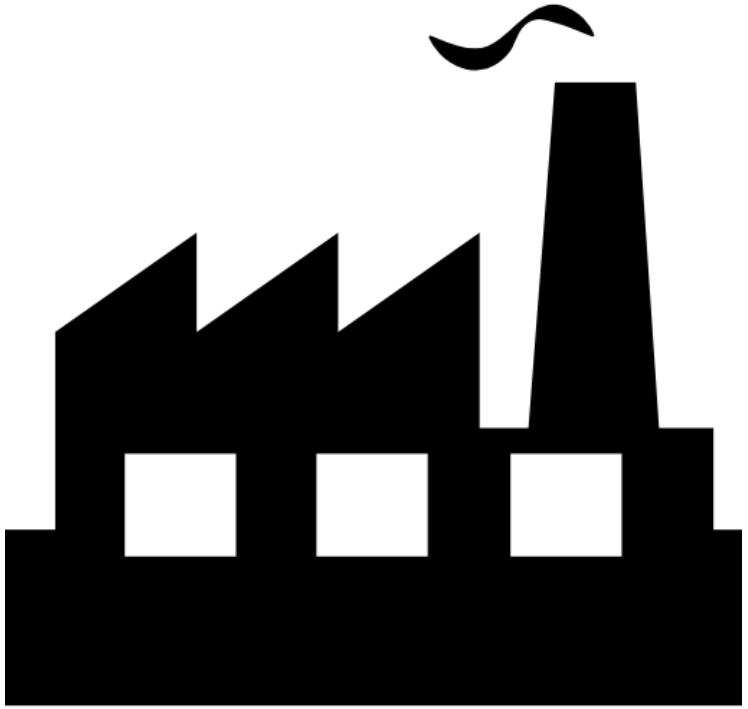
Growing IT Department

Tons of Infosec Jobs

CYMOTIVE
TECHNOLOGIES


VEHICLES
HACKERS
HACKERS

Some Terminology

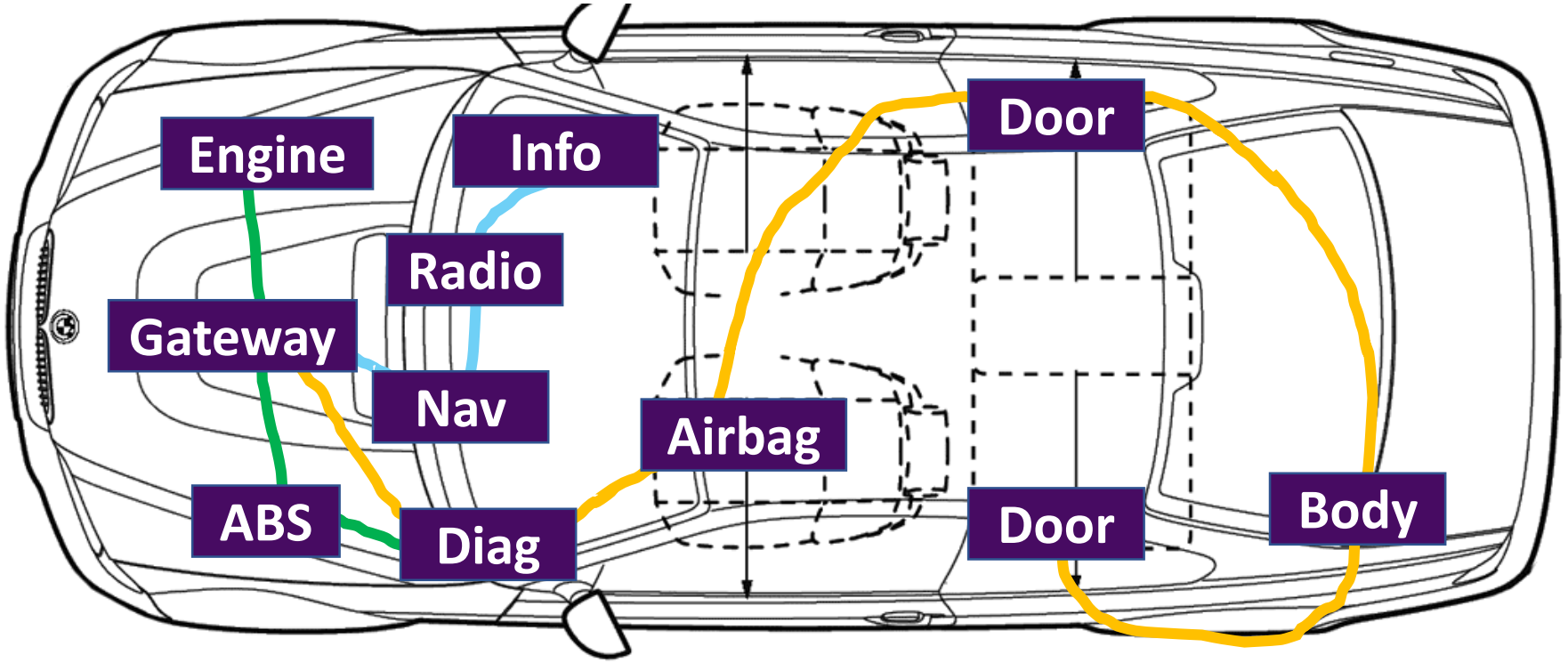


Original Equipment Manufacturer (OEM)

CYMOTIVE TECHNOLOGIES

Some Terminology

Electronic Control Unit (ECU)

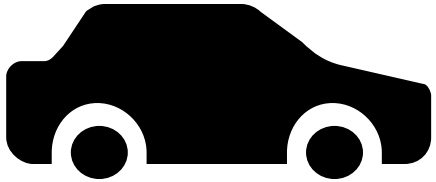


Some Terminology

Infotainment (Information + Entertainment)

Progress Bar

- ~~Who We Are~~
- ~~Automotive Past & Future~~
- Connected Technologies
- Centralized Management



CYMOTIVE TECHNOLOGIES

The new fashion in vehicle IoT are “Aftermarket Solutions”

Which are also the solution for hackers

CYMOTIVE TECHNOLOGIES

Aftermarket Solutions

Chainway TSP

Samsung

Vinli OBD-II

Engie

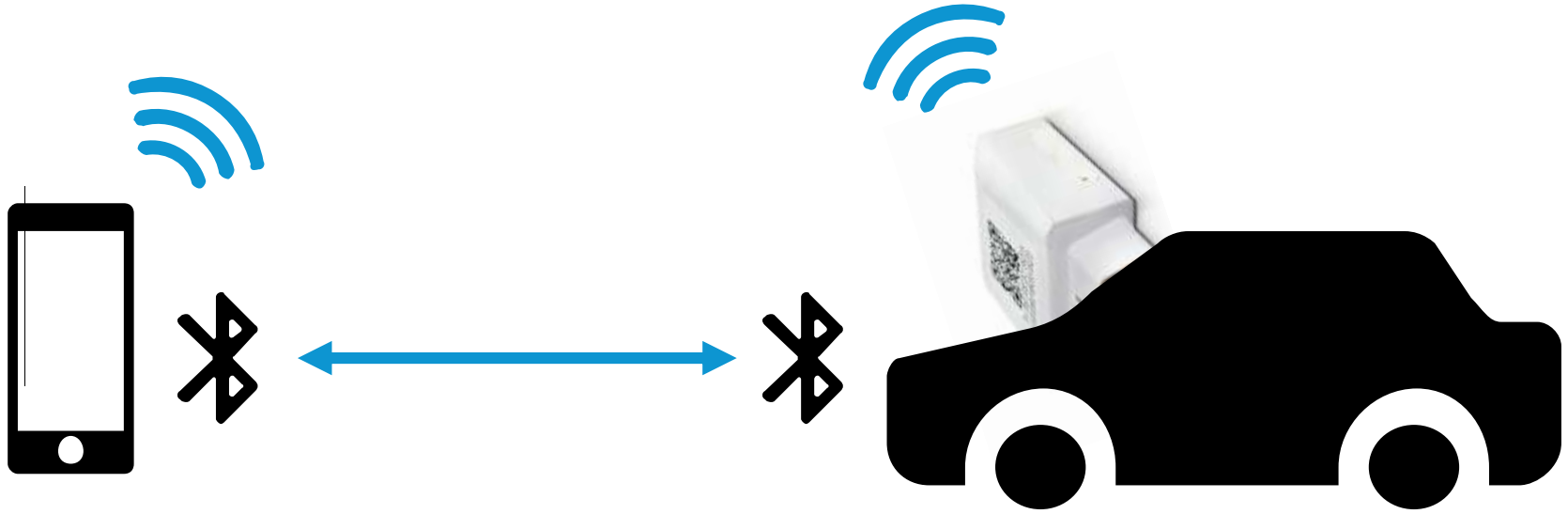
Viper Smart Start

Drone Mobile

MYCAR

CYMOTIVE TECHNOLOGIES

Hacking the:
Server, Phone, Dongle
->
Hacking the car



CYMOTIVE TECHNOLOGIES

Keyless Entry =< Car Sharing

MyCar

CAR 2GO

By Continental
https://www.youtube.com/watch?v=vdnrr5i4naE

ANDY GREENBERG SECURITY 08.10.19 02:50 PM

A REMOTE-START APP EXPOSED THOUSANDS OF CARS TO HACKERS

MYCAR App - Found by Jmaxxz

More Than 100 High-End Cars Were Stolen Using An App In A Possible Chicago Crime Spree

All 100 vehicles, including at least 50 Mercedes-Benz cars, that were reported missing are being recovered, the company said on Thursday.

Stephanie K. Baer
BuzzFeed News Reporter

Last updated on April 18, 2019, at 10:48 a.m. ET
Posted on April 17, 2019, at 9:34 p.m. ET

Car2Go App

CYMOTIVE TECHNOLOGIES

The Bluetooth Problem

Infotainment, Dongles, Keys are all Bluetooth connected

Hell2CAP (Cymotive)
CVE-2018-20378

KNOB (SUTD)
CVE-2019-9506

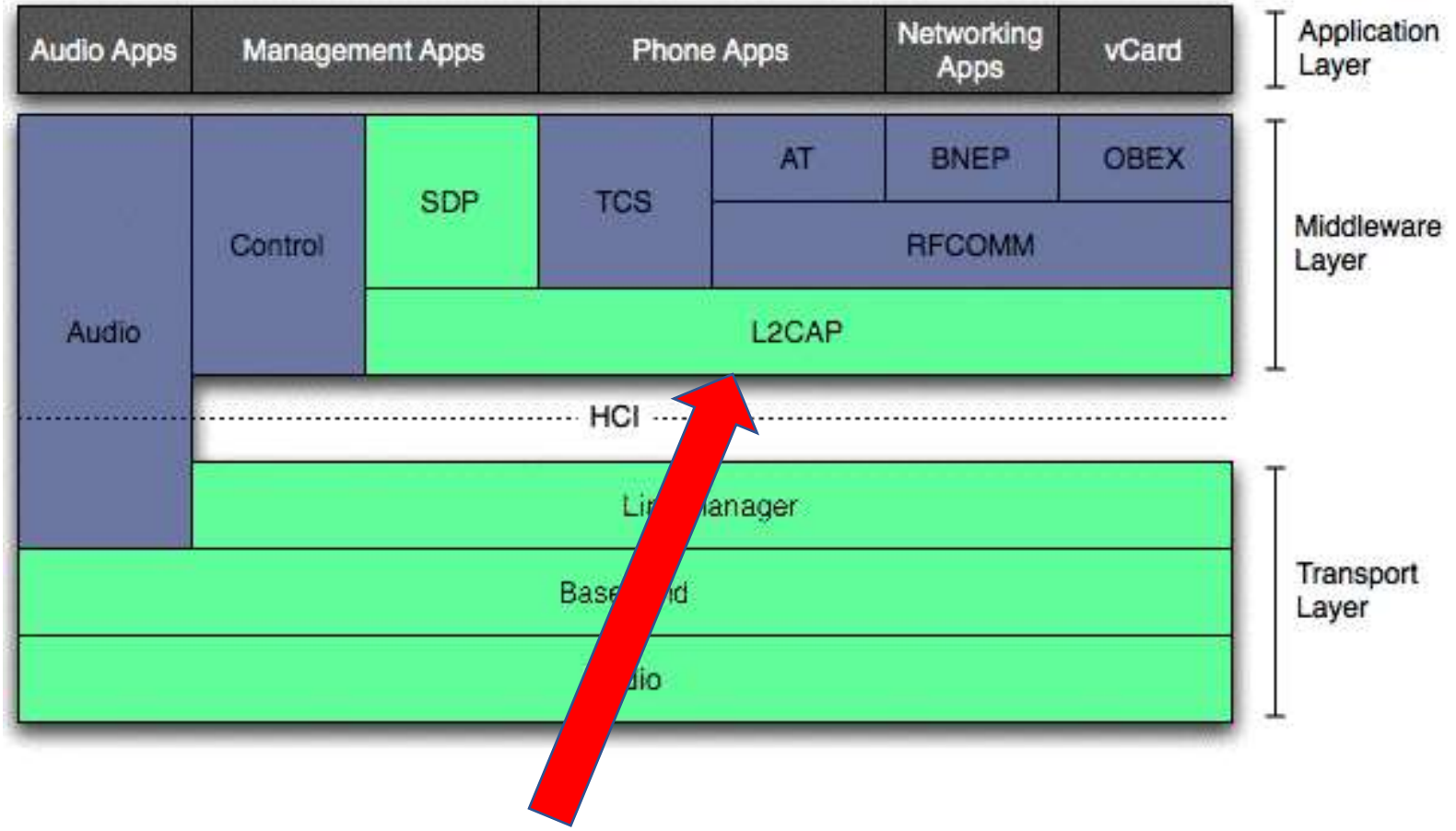
BleedingBit (Armis)
CVE-2018-16986
CVE-2018-7080

CYMOTIVE TECHNOLOGIES

Hell2CAP

Found by **Barak Caspi** at Cymotive

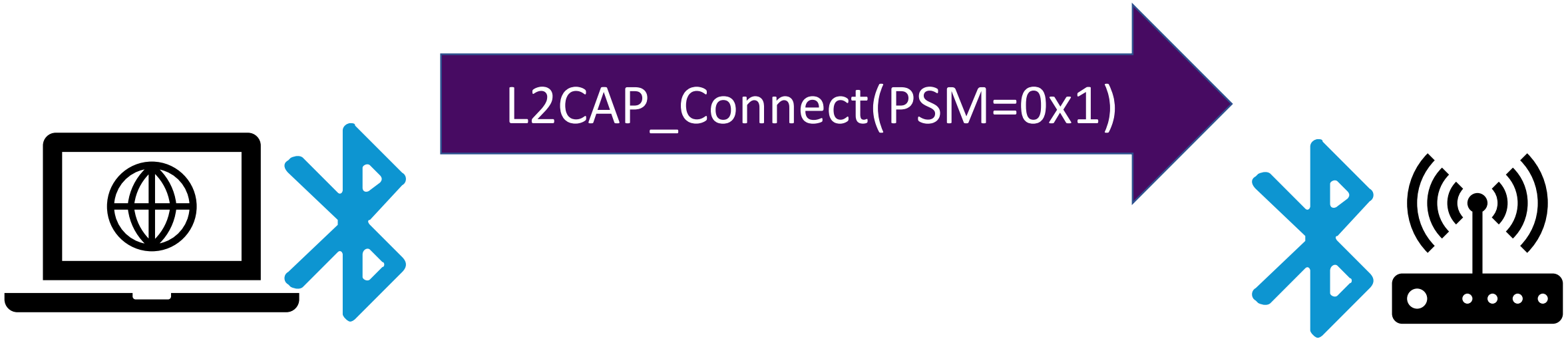
State machine bug in BlueSDK L2CAP (~100 Million Devices)



CYMOTIVE TECHNOLOGIES

L2CAP Channel Multiplexing

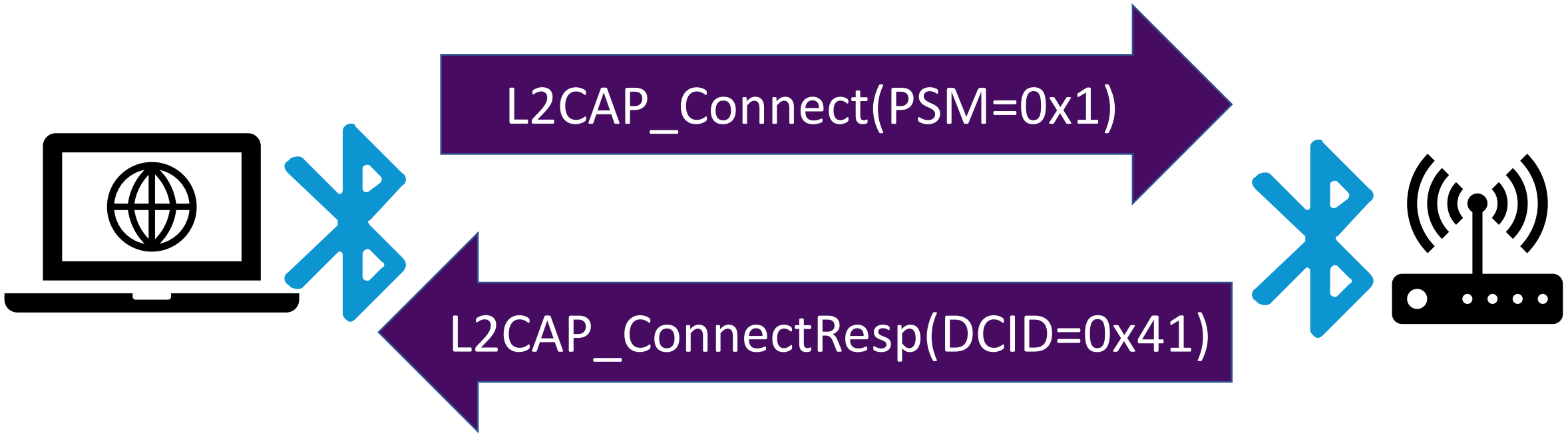
PSM – “Protocol ID”



L2CAP Channel Multiplexing

PSM – “Protocol ID”

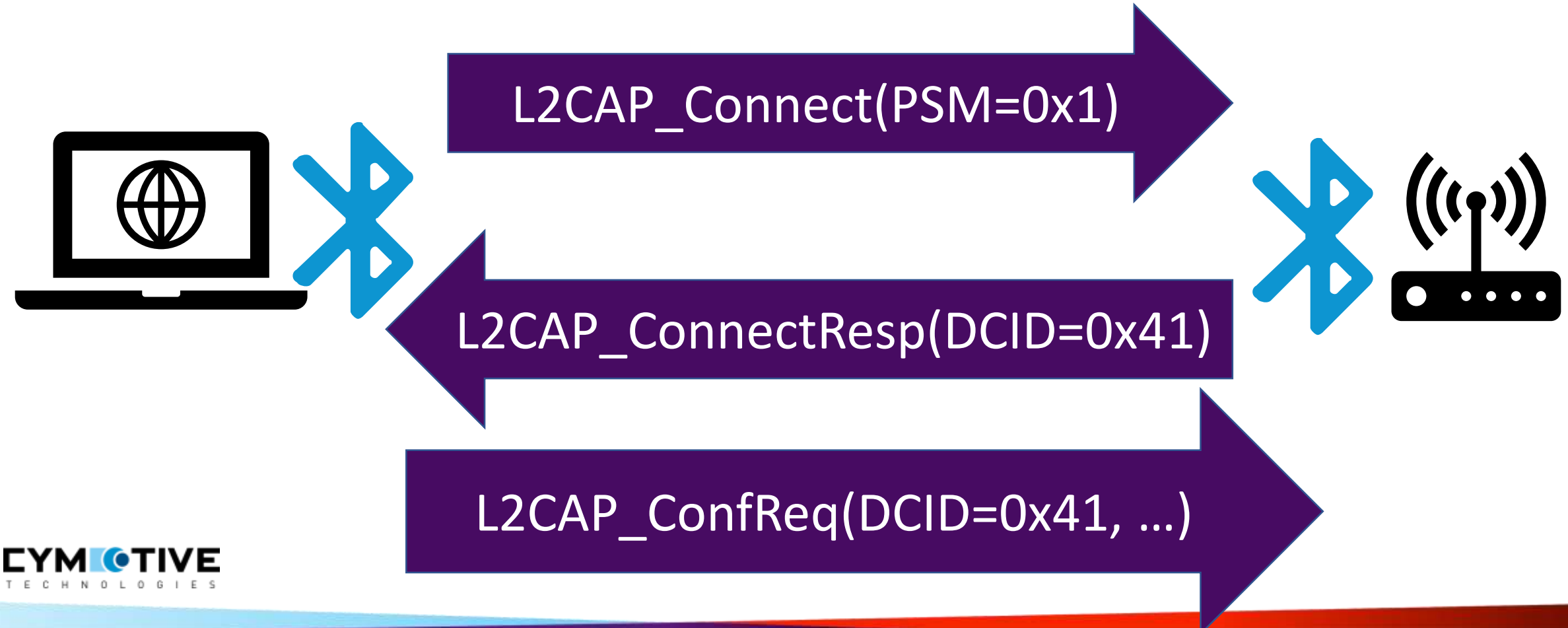
DCID – channel identifier



L2CAP Channel Multiplexing

PSM – “Protocol ID”

DCID – channel identifier



L2CAP Configuration

Can config: MTU, Timeout and more

Minimal Bluetooth MTU is 48

local device can receive, in this channel, an MTU larger than the minimum required. All L2CAP implementations shall support a minimum MTU of 48 octets, however some protocols and profiles explicitly require support for a

- Bluetooth Specification Version 3.0 + HS [Vol 3]

L2CAP Configuration

```
1  if ( config_option[1] == ConfigOption_MTU )
2  {
3    in_mtu = LEtoHost16(data_iter + 2);
4    channel->MTU = in_mtu;
5    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu )
6    {
7      l2cap_set_channel_as_invalid(channel);
8    }
9  }
```

Pseudo code

Save MTU

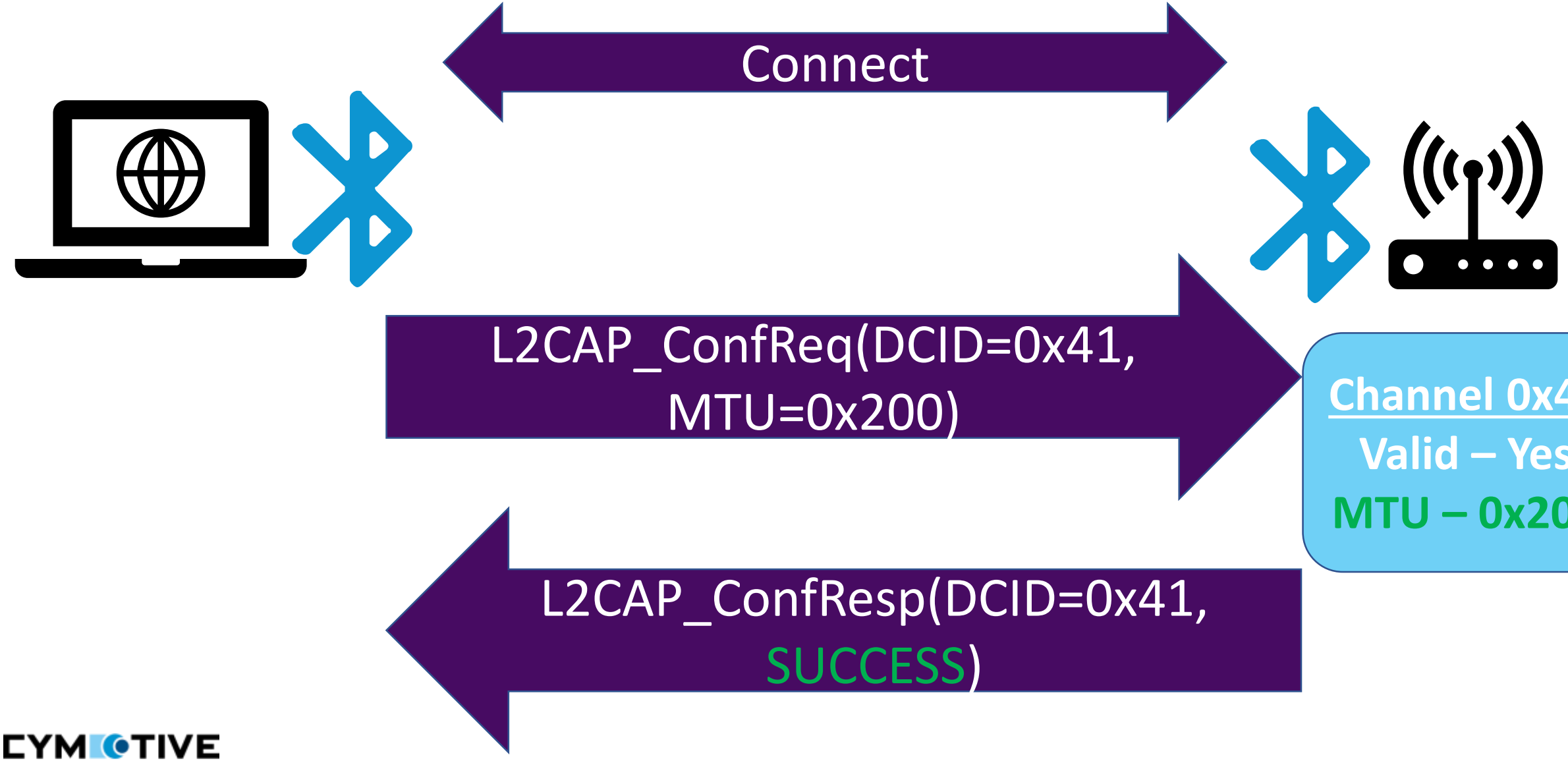
Set Invalid
On Fail

Check Size

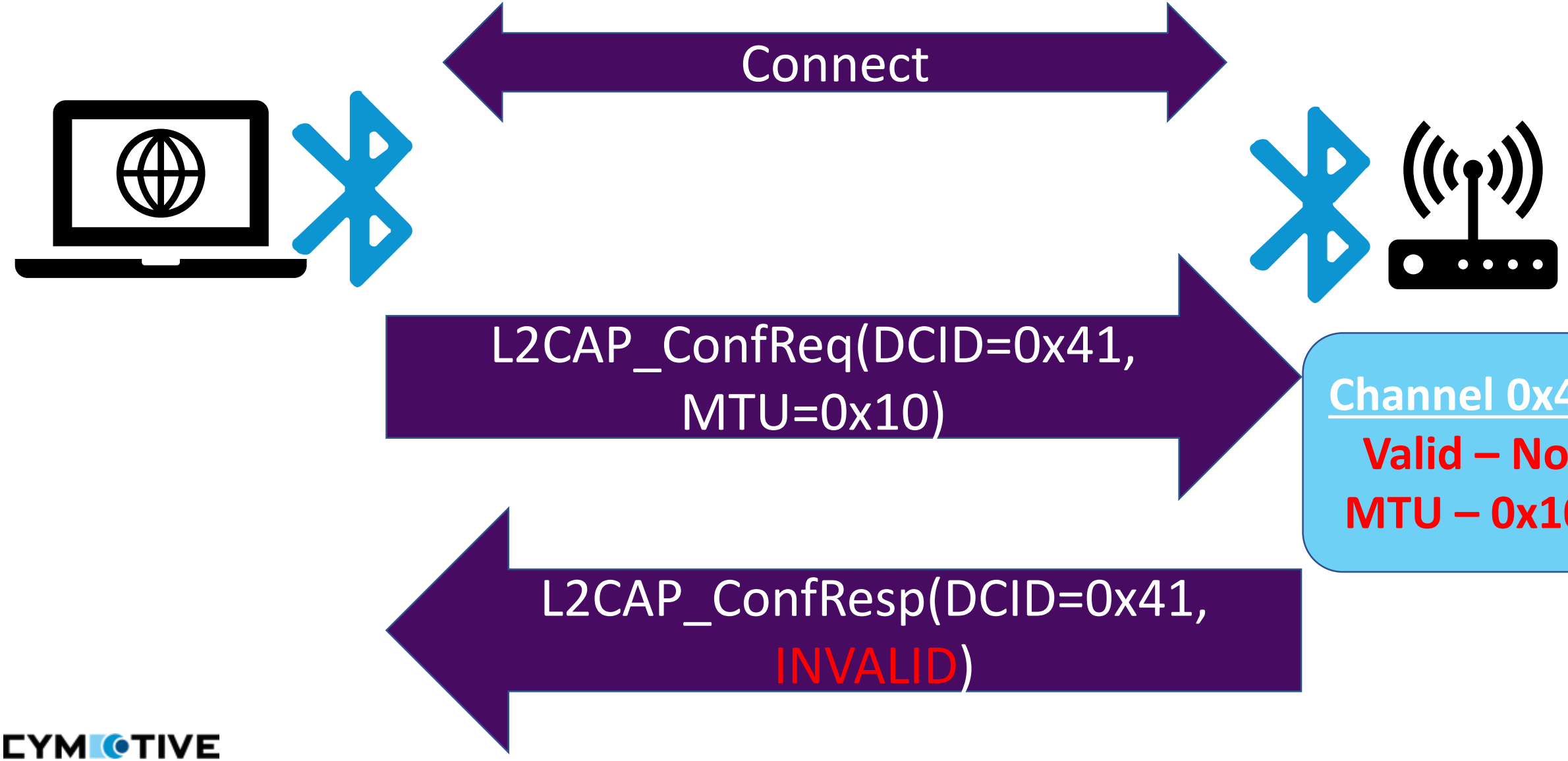
CYMOTIVE TECHNOLOGIES

L2CAP Configuration

L2CAP Configuration



L2CAP Configuration



Hell2CAP

Red flag – Values is stored (4) than checked (5)

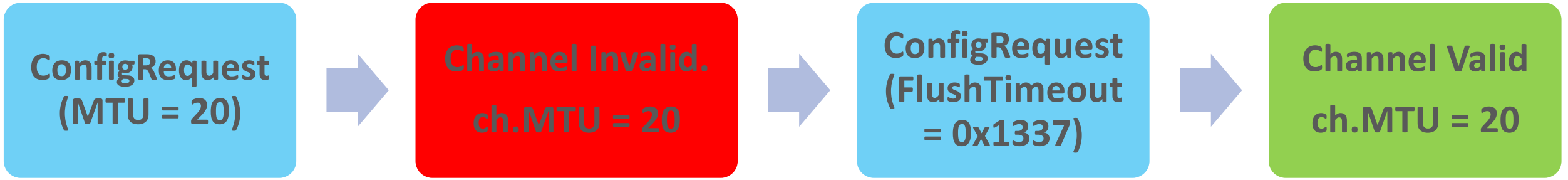
Can we restore channel to be valid?

```
1  if ( config_option[1] == ConfigOption_MTU )
2  {
3    in_mtu = LEtoHost16(data_iter + 2);
4    channel->MTU = in_mtu;
5    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu )
6    {
7      l2cap_set_channel_as_invalid(channel);
8    }
9  }
```

Hell2CAP

Red flag – Values is stored (4) than checked (5)

Can we restore channel to be valid?



Hell2CAP

On upper layer – SDP there is fragmentation code

```
1  MTU = L2CAP_GetTxMtu(_sdpInfo->CID);
2  availableSizeForFragment = (MTU - 9) & 0xFFFF;
3  ...
4  SdpStoreAttribData(_sdpInfo, _txPkt, _txPkt->bufferPtr, availableSizeForFragment);
```

MTU from L2CAP, we control it

Hell2CAP

On upper layer – SDP there is fragmentation code

```
1  MTU = L2CAP_GetTxMtu(_sdpInfo->CID);
2  availableSizeForFragment = (MTU - 9) & 0xFFFF;
3  ...
4  SdpStoreAttribData(_sdpInfo, _txPkt, _txPkt->bufferPtr, availableSizeForFragment);
```

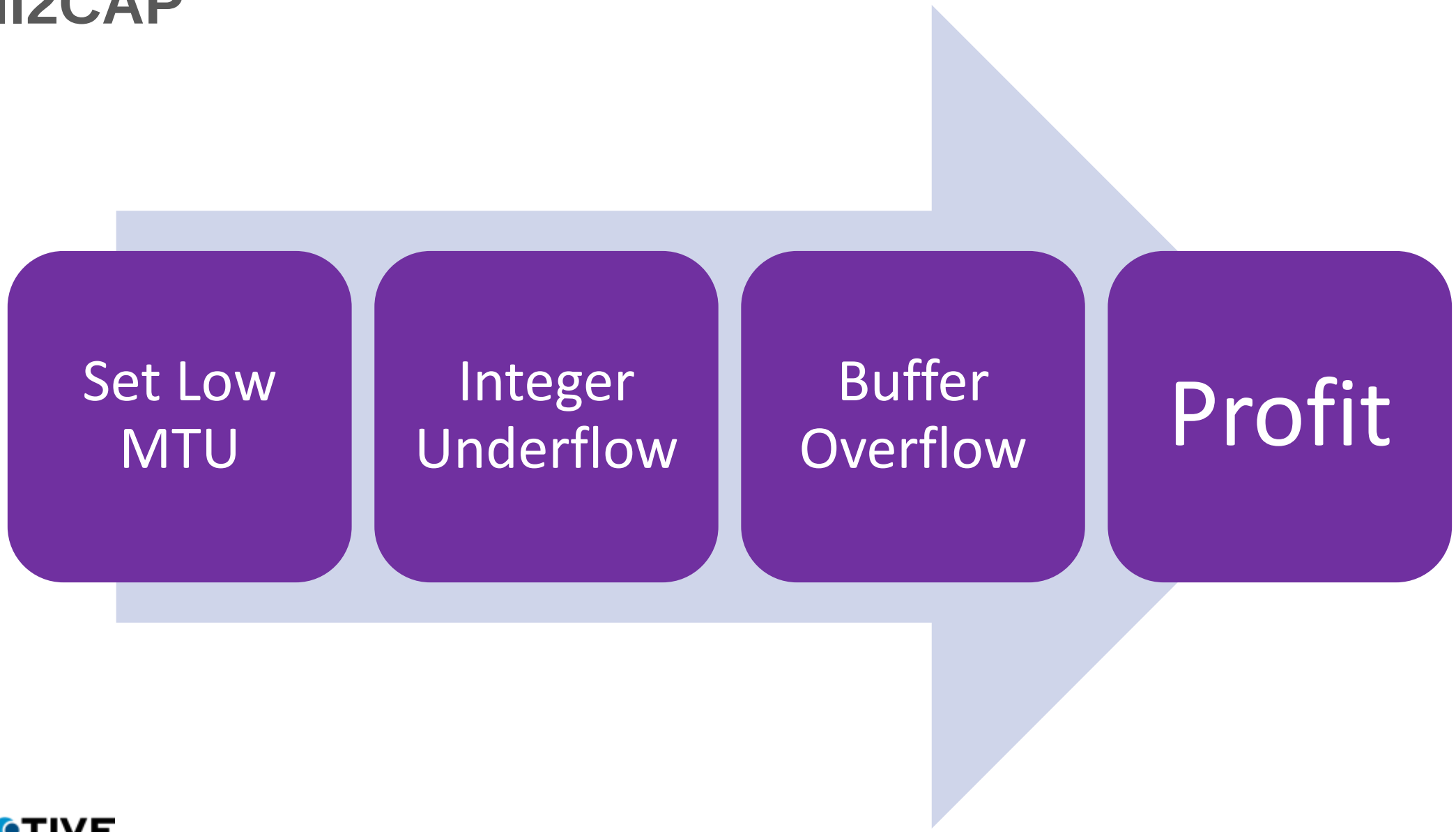
MTU = 48 -> availableSizeForFragment = 48 – 9 = 39

MTU = 8 -> availableSizeForFragment = 8 – 9 = **0xFFFF**

Integer underflow

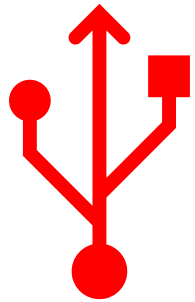
CYMOTIVE TECHNOLOGIES

Hell2CAP

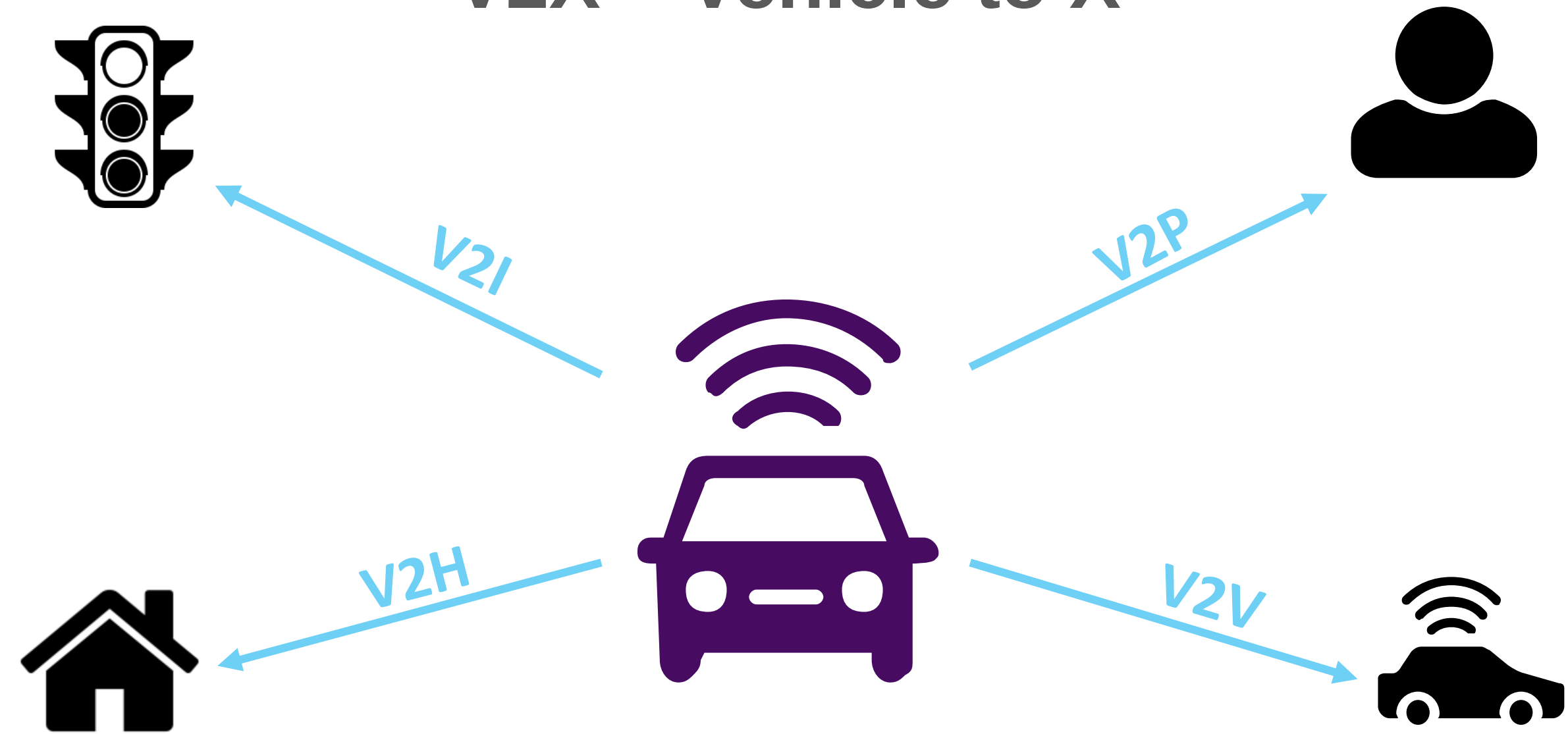


The problem with Bluetooth is that it is not the only problem

V2X



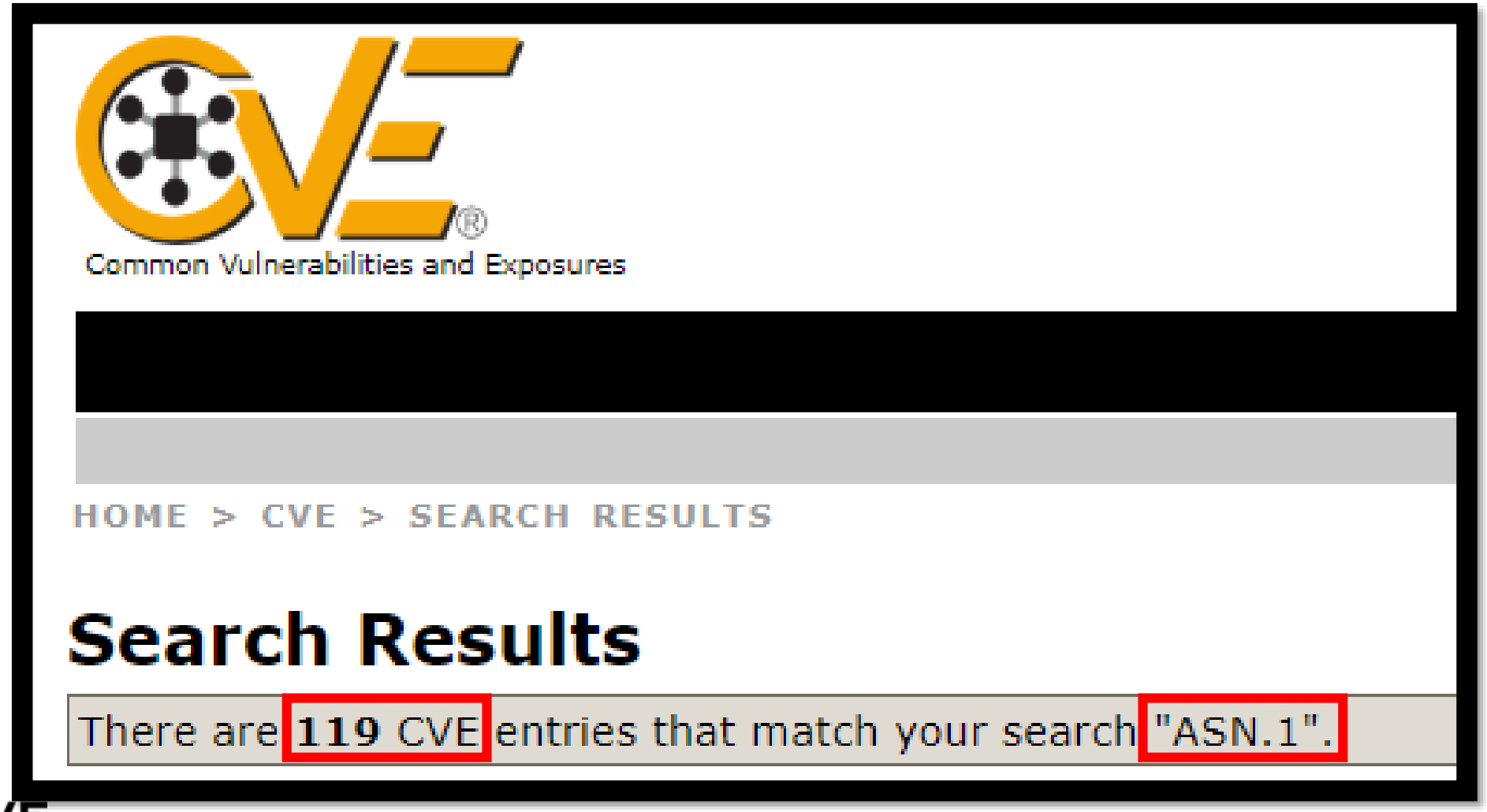
V2X – Vehicle to X



CYMOTIVE TECHNOLOGIES

By Autotalks
https://www.youtube.com/watch?v=RRDiDPnv_b4

V2X payload is ASN.1 based

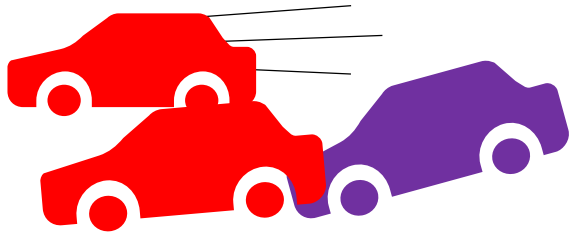


CYMOTIVE TECHNOLOGIES

A fake V2X module could

Create False Traffic

Force Emergency Breaks



Generate False Alarms

CYMOTIVE TECHNOLOGIES

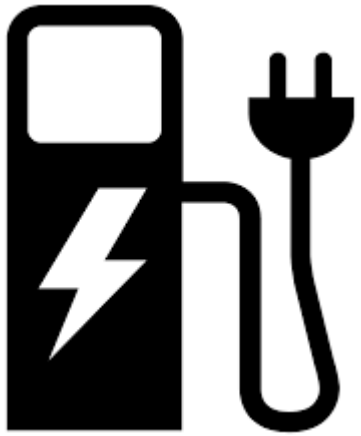
Charging Evolution

CYMOTIVE TECHNOLOGIES

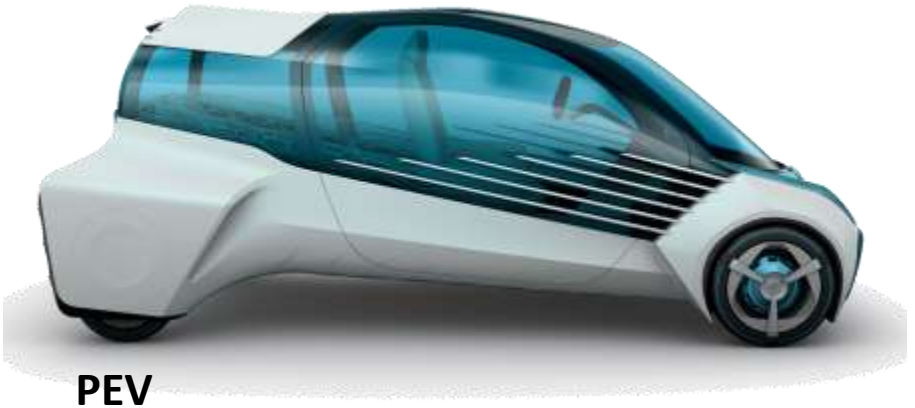
Charging PLC

EVSE – Electric Vehicle Supply Equipment

PEV – Plug-in Electric Vehicle



EVSE

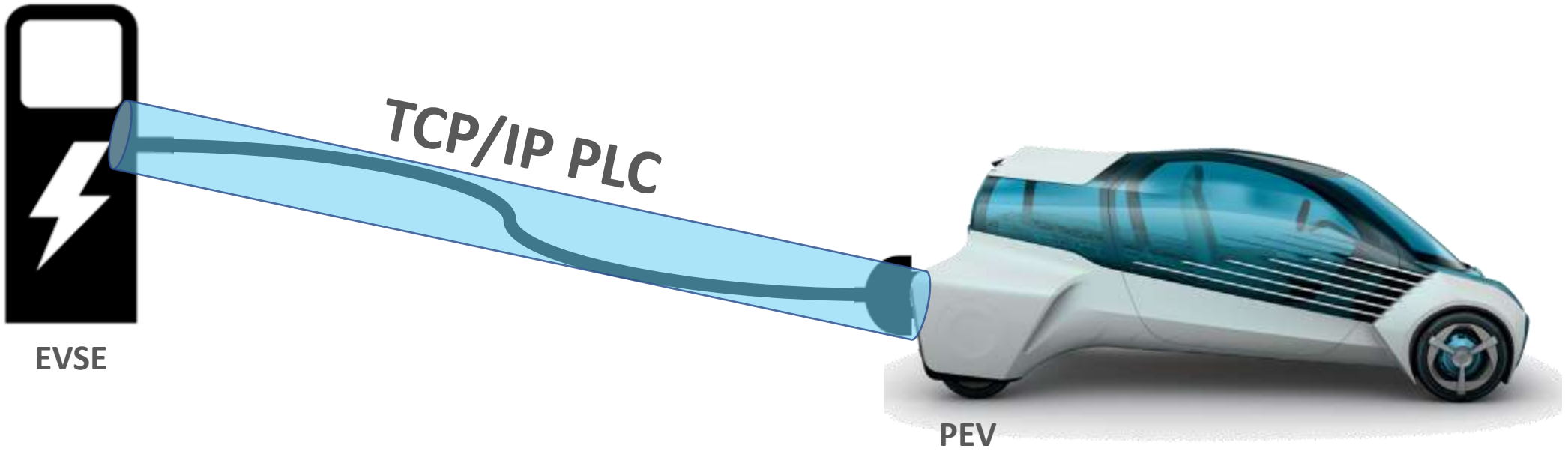


PEV

CYMOTIVE TECHNOLOGIES

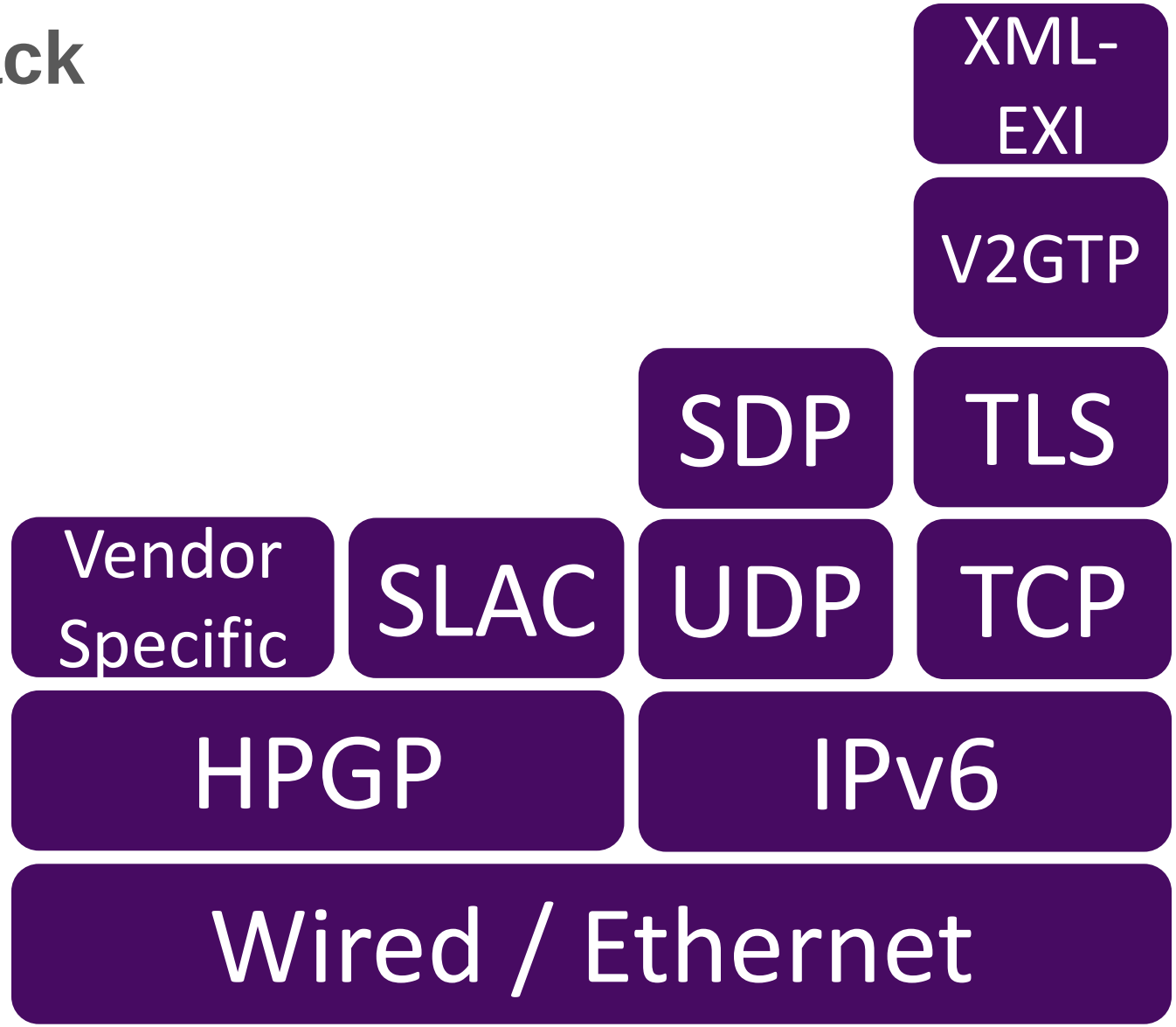
Charging PLC

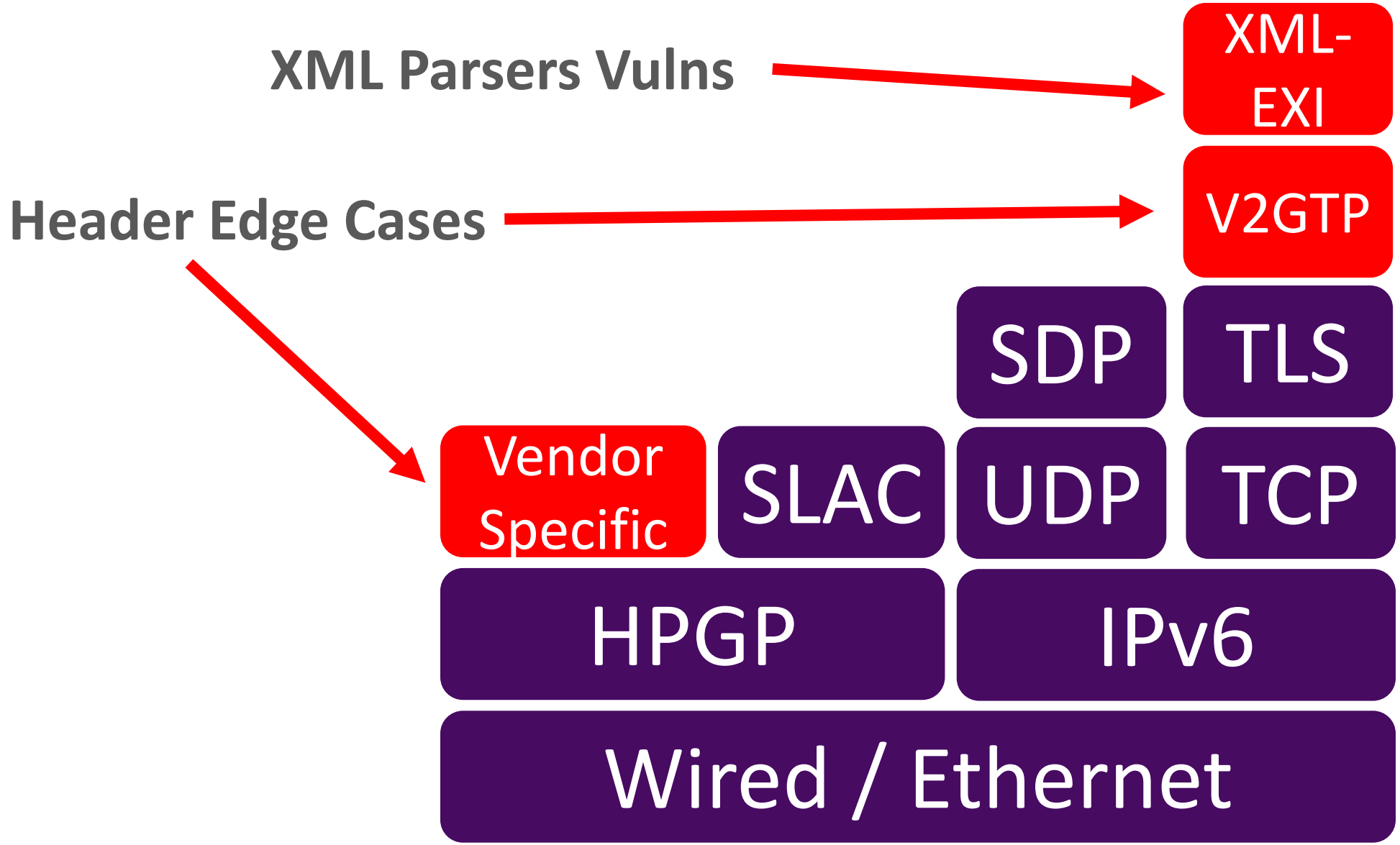
PLC – Power Line Communication

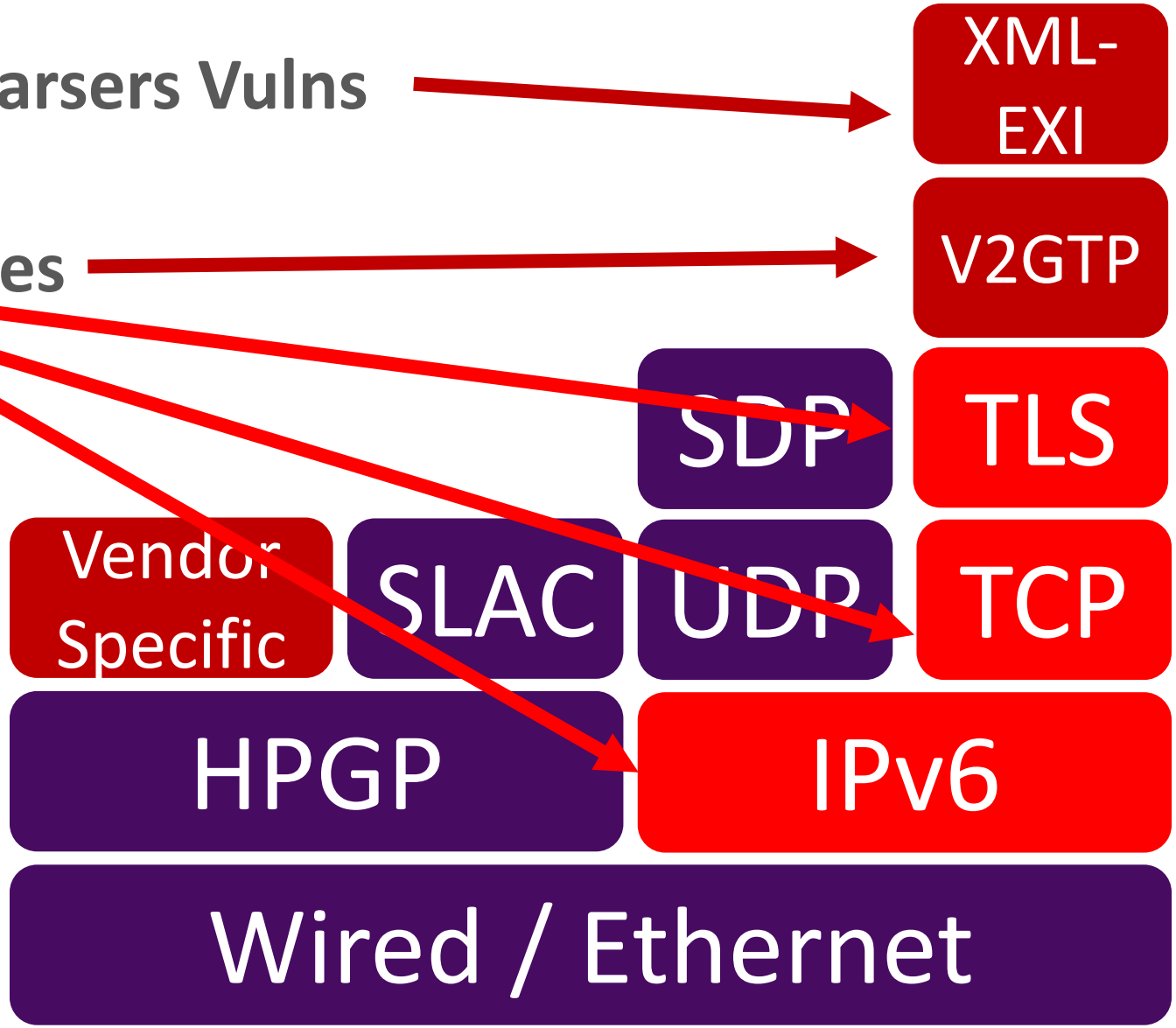


CYMOTIVE TECHNOLOGIES

Charging Protocol Stack




XML Parsers Vulns
XML-EXI
Header Edge Cases
V2GTP
SDP
TLS
Vendor Specific
SLAC
UDP
TCP
HPGP
IPv6
Wired / Ethernet



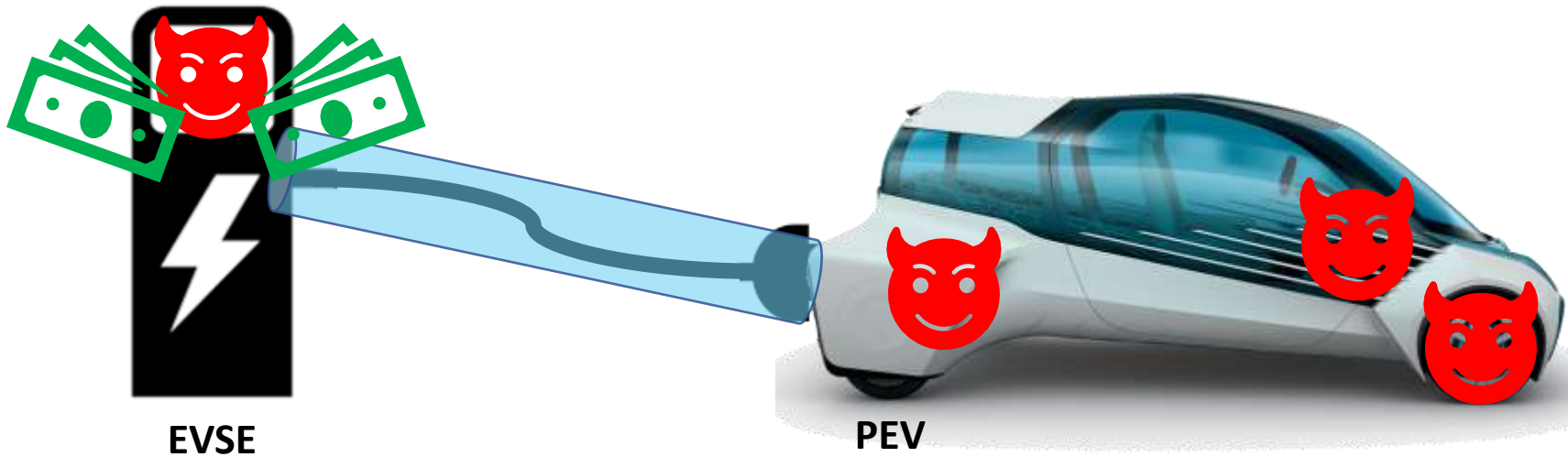
VxWorks TCP/IP Stack CVEs by Armis Labs URGENT/11 (19.7.2019):
IP RCE: CVE-2019-12256
TCP RCE: CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263

EVSE! Use Buffer Overflow!

Hackers Benefits

Charge your credit card and not your car

Hack other ECUs from PEV



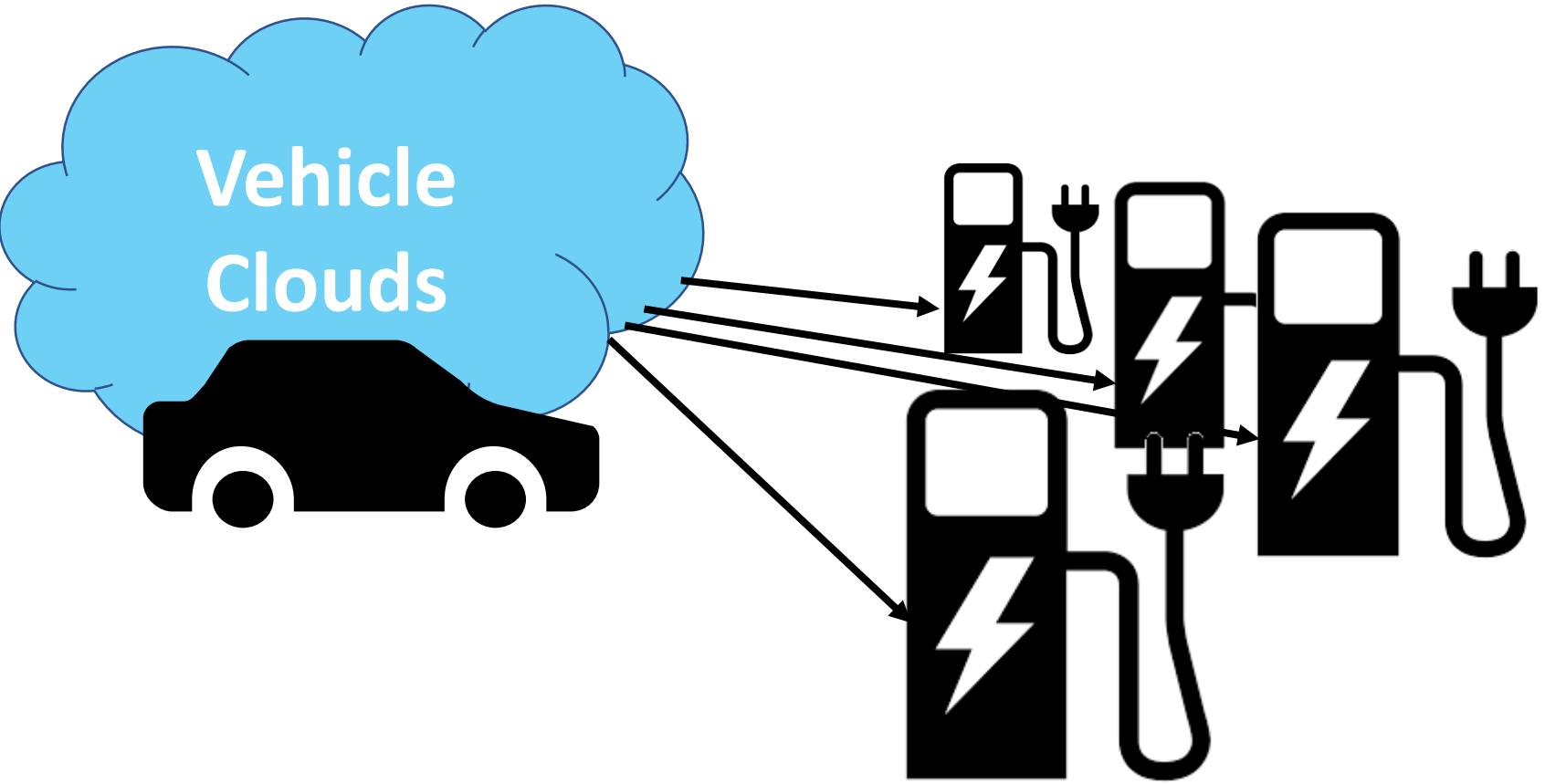
CYMOTIVE TECHNOLOGIES

Progress Bar

- ~~Who I Am~~
- ~~Automotive Past & Future~~
- ~~Connected Technologies~~
- Centralized Management

CYMOTIVE TECHNOLOGIES

Hackers Benefits



EVSEs are all cloud connected

The Magical Place Where Everything Is Possible

(For a Hacker)

CYMOTIVE TECHNOLOGIES

Normal Stuff

Private Information

Credit Cards

OEM Secrets

Juicy Stuff

GPS Coordinates

Remote Unlock

OTA Updates

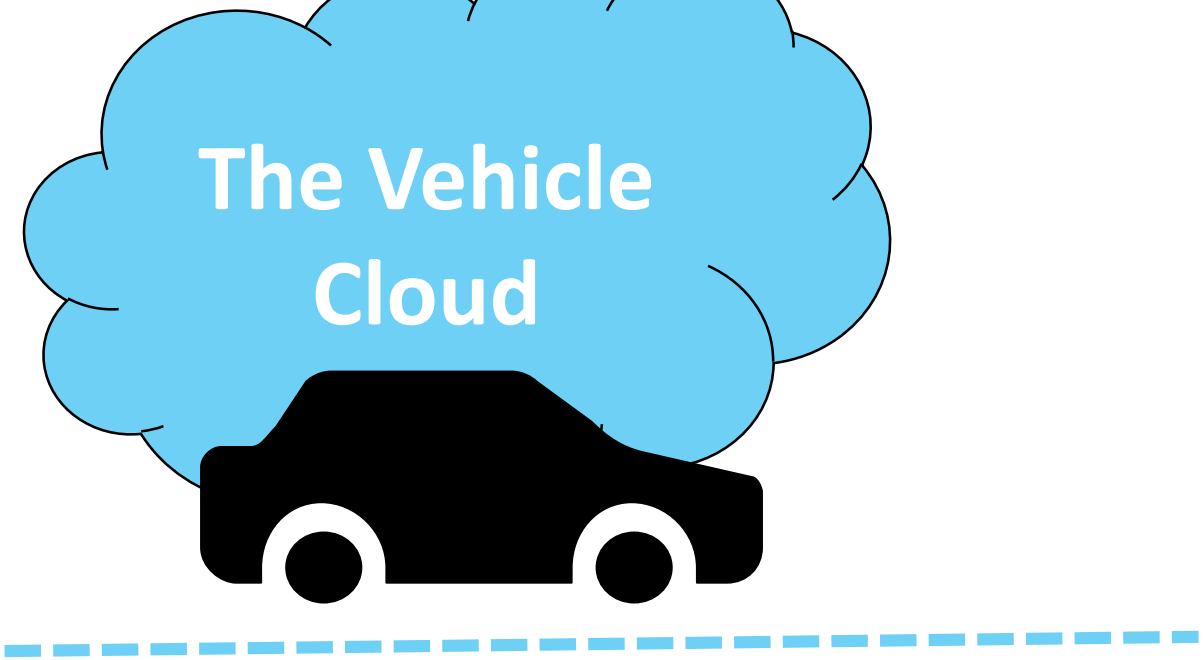
CYMOTIVE
TECHNOLOGIES

Futuristic Stuff

Centralized Control for Shared Transportation

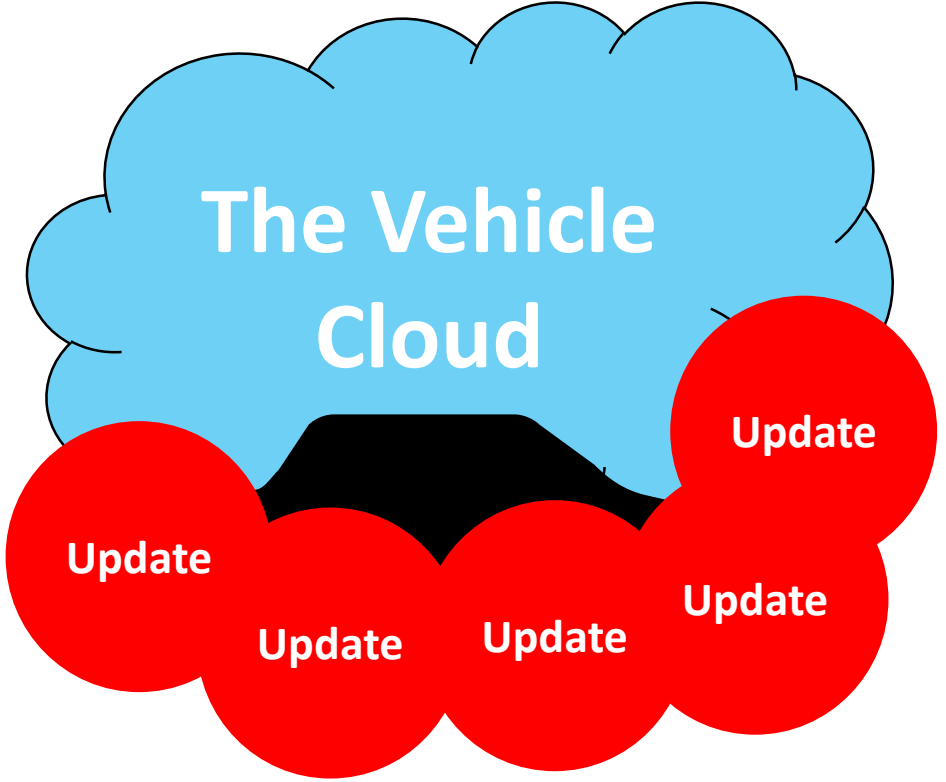
Next-Gen Police

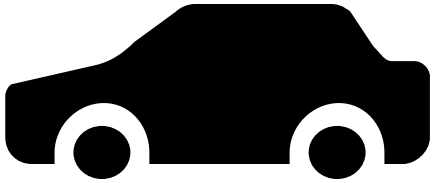
The cloud is the limit…



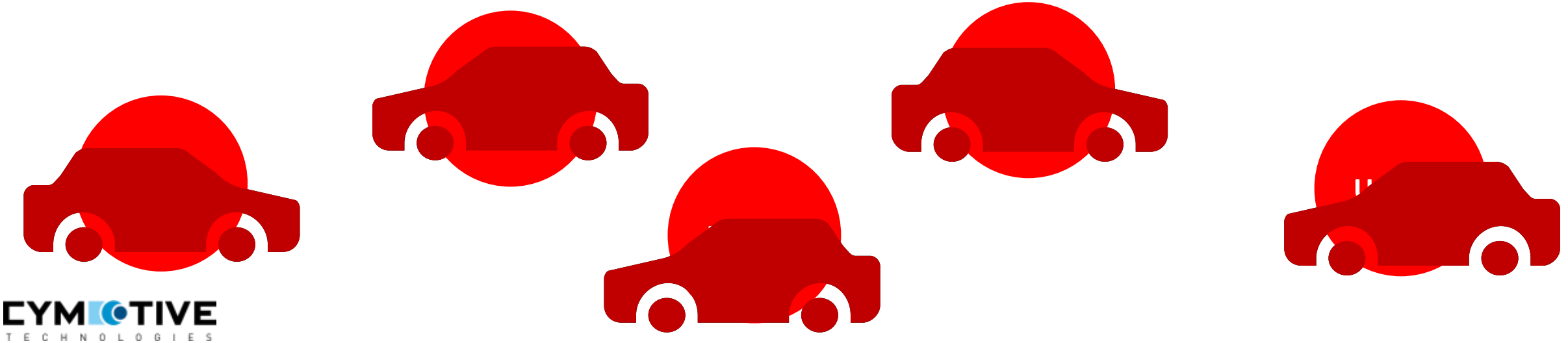
OTA – Over The Air

Most modern cars receive software updates with 4G connection to the OEM servers





CYMOTIVE TECHNOLOGIES



CYMOTIVE
TECHNOLOGIES


MENU
MAP
AUDIO
VOL
PUSH
CAMERA
BACK
TUNE·SCROLL
PUSH
SOUND
STOP!
Pay 5000$ to
unlock this car

How I hacked Volkswagen and Skoda.
A story about Volkswagen Group Car Remote Hacking.

This article is a responsible disclosure case study of reporting vulnerabilities found in production systems of a Giant Company that doesn't (yet?) have a Bug Bounty program.

Who Am I

My name is Daniel Rękawek.
I am a Cyber Security Consultant, Pentester and IT/Security enthusiast.
Located in Poland, always happy to travel.
Please find my **LinkedIn profile.**
Interested in collaboration? **Contact me.**

4/11/2019

The bright side

OEMs invest immense efforts in cyber security

Connected autonomous would be really great

TL;DR

Risks

Everything Is Connected

New Attack Vectors – BT, Wifi, NFC, V2X, PLC

Opportunities

Less Accidents

Life Changing Technologies

CYMOTIVE TECHNOLOGIES

Ask Me Anything

Lior.yaari@cymotive.com

Website

Lior@imperium-sec.com

LinkedIn

Twitter: @lior_yaari

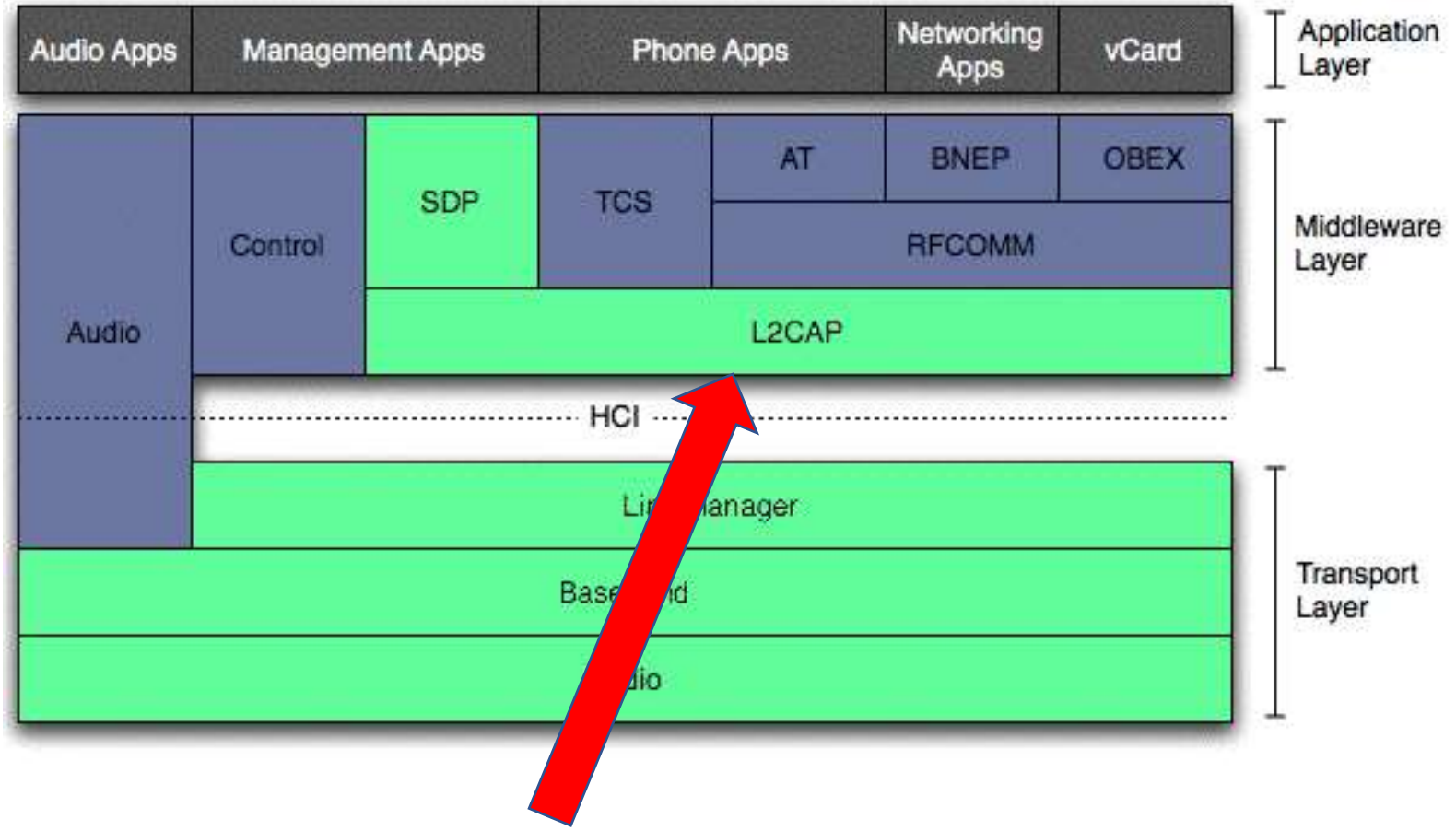
CYMOTIVE TECHNOLOGIES

DEEPSEC

Hell2CAP

Found by Barak Caspi at Cymotive

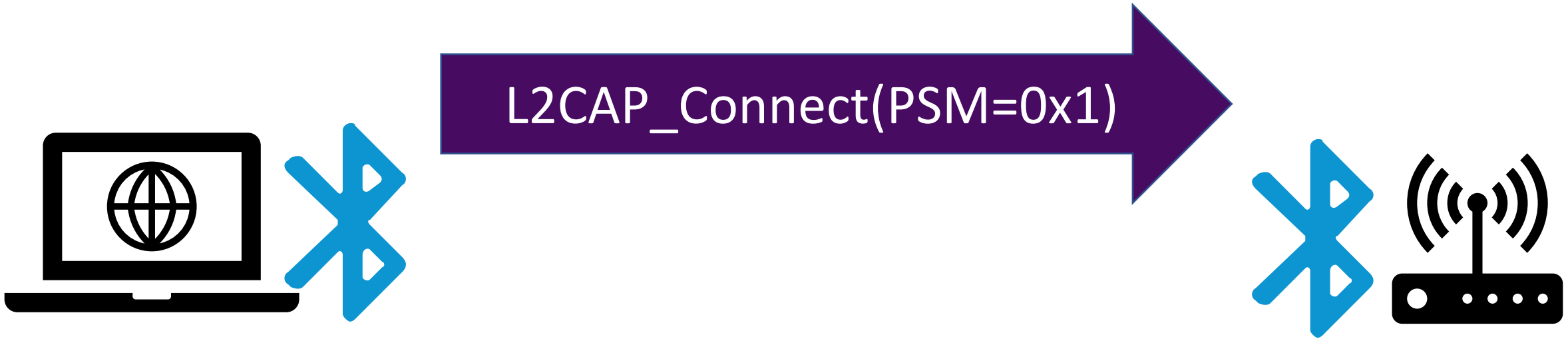
State machine bug in BlueSDK L2CAP (~100 Million Devices)



CYMOTIVE TECHNOLOGIES

L2CAP Channel Multiplexing

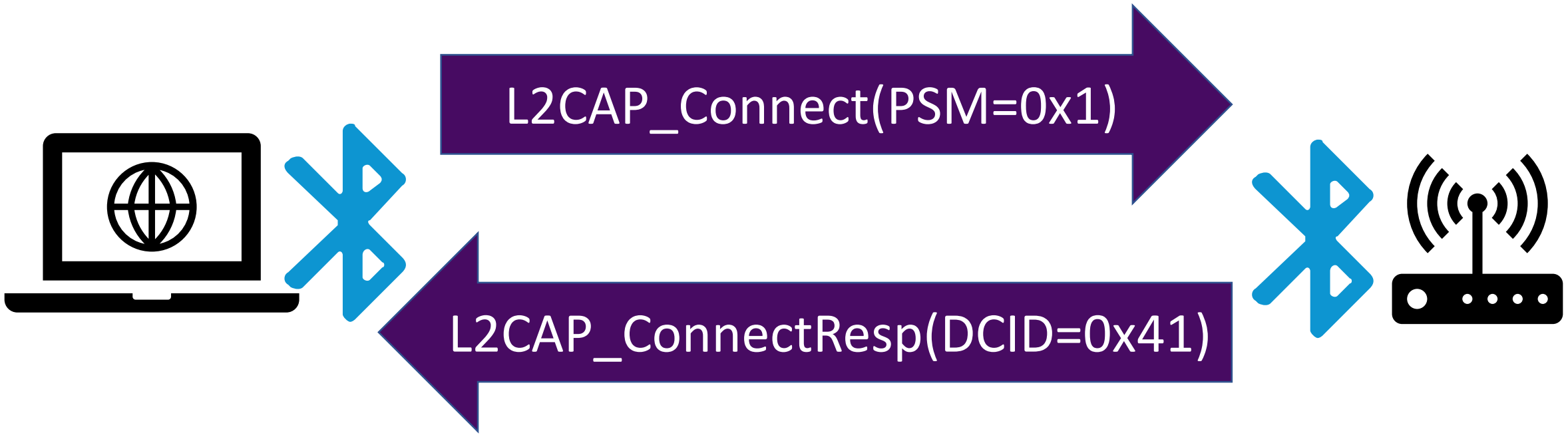
PSM – “Protocol ID”



L2CAP Channel Multiplexing

PSM – “Protocol ID”

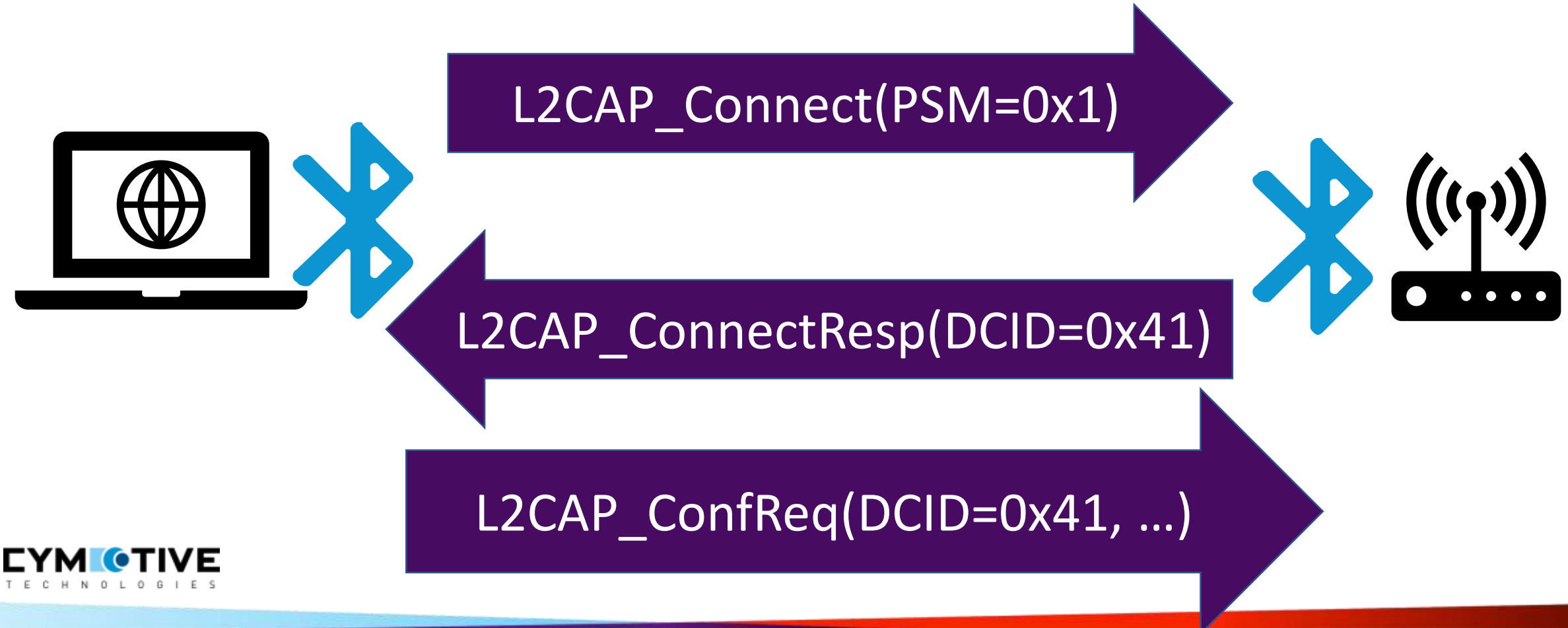
DCID – channel identifier



L2CAP Channel Multiplexing

PSM – “Protocol ID”

DCID – channel identifier



L2CAP Configuration

Can config: MTU, Timeout and more

Minimal Bluetooth MTU is 48

local device can receive, in this channel, an MTU larger than the minimum required. All L2CAP implementations shall support a minimum MTU of 48 octets, however some protocols and profiles explicitly require support for a

- Bluetooth Specification Version 3.0 + HS [Vol 3]

L2CAP Configuration

```
1  if ( config_option[1] == ConfigOption_MTU )
2  {
3    in_mtu = LEtoHost16(data_iter + 2);
4    channel->MTU = in_mtu;
5    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu )
6    {
7      l2cap_set_channel_as_invalid(channel);
8    }
9  }
```

Pseudo code

Save MTU

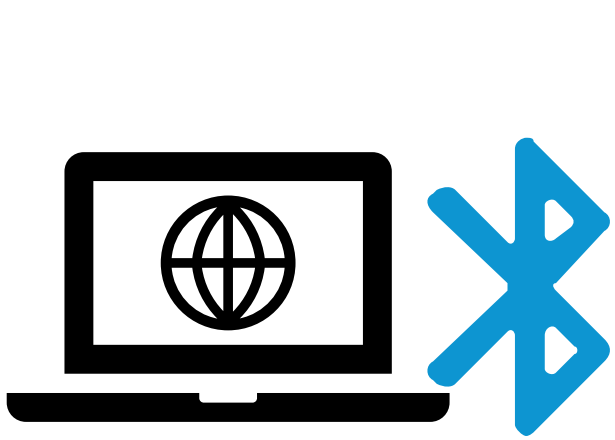
Set Invalid
On Fail

Check Size

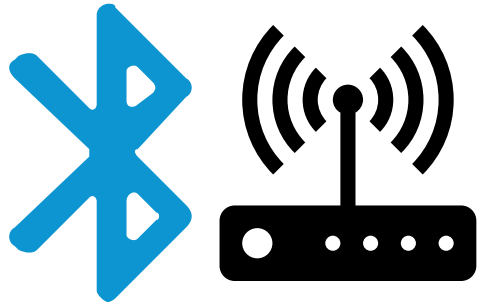
CYMOTIVE TECHNOLOGIES

L2CAP Configuration

L2CAP Configuration



Connect



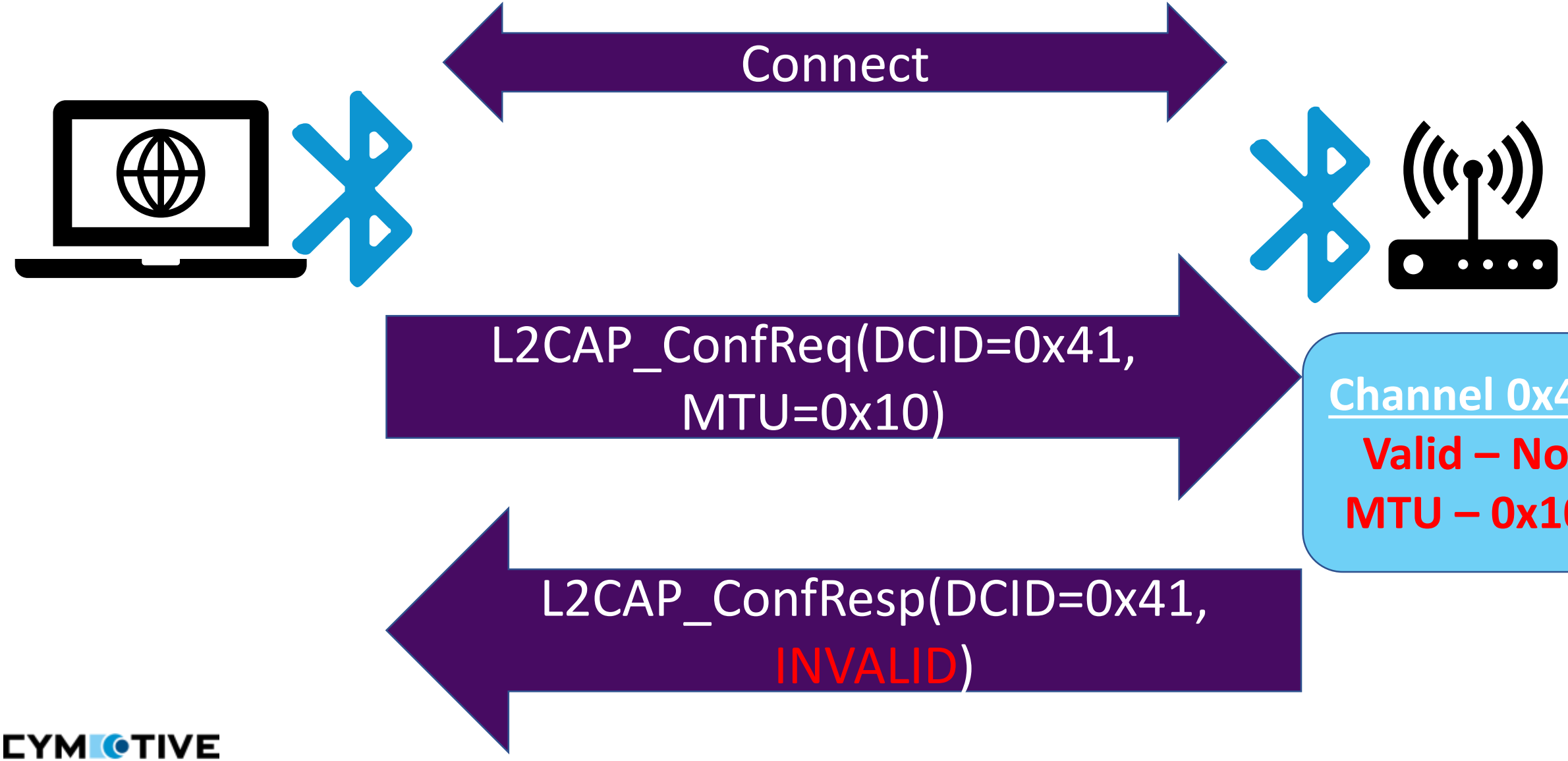
L2CAP_ConfReq(DCID=0x41, MTU=0x200)

Channel 0x41
Valid – Yes
MTU – 0x200

L2CAP_ConfResp(DCID=0x41, SUCCESS)

CYMOTIVE TECHNOLOGIES

L2CAP Configuration



Hell2CAP

Red flag – Values is stored (4) than checked (5)

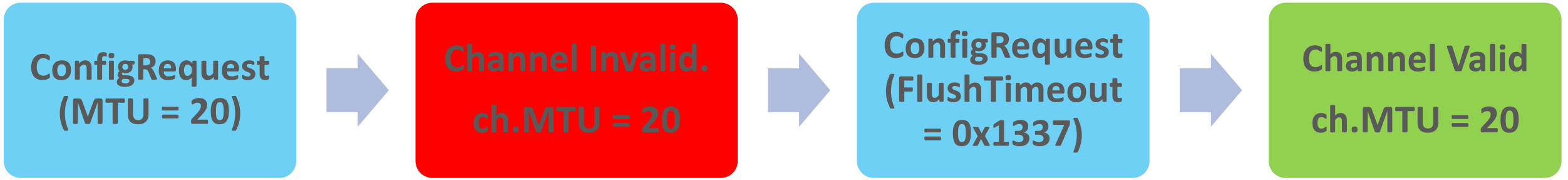
Can we restore channel to be valid?

```
1  if ( config_option[1] == ConfigOption_MTU )
2  {
3    in_mtu = LEtoHost16(data_iter + 2);
4    channel->MTU = in_mtu;
5    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu )
6    {
7      l2cap_set_channel_as_invalid(channel);
8    }
9  }
```

Hell2CAP

Red flag – Values is stored (4) than checked (5)

Can we restore channel to be valid?



Hell2CAP

On upper layer – SDP there is fragmentation code

```
1  MTU = L2CAP_GetTxMtu(_sdpInfo->CID);
2  availableSizeForFragment = (MTU - 9) & 0xFFFF;
3  ...
4  SdpStoreAttribData(_sdpInfo, _txPkt, _txPkt->bufferPtr, availableSizeForFragment);
```

MTU from L2CAP, we control it

Hell2CAP

On upper layer – SDP there is fragmentation code

```
1  MTU = L2CAP_GetTxMtu(_sdpInfo->CID);
2  availableSizeForFragment = (MTU - 9) & 0xFFFF;
3  ...
4  SdpStoreAttribData(_sdpInfo, _txPkt, _txPkt->bufferPtr, availableSizeForFragment);
```

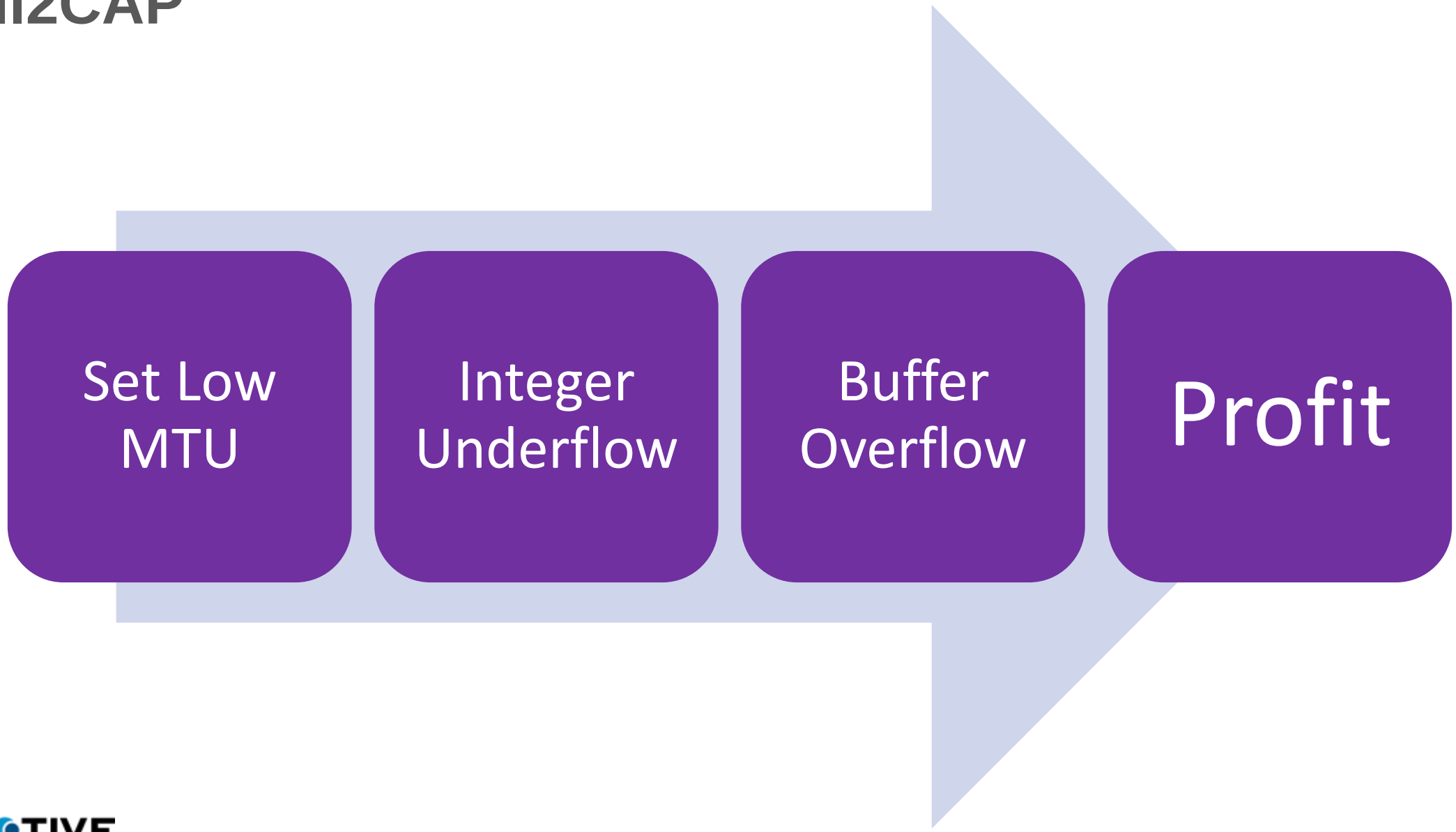
MTU = 48 -> availableSizeForFragment = 48 – 9 = 39

MTU = 8 -> availableSizeForFragment = 8 – 9 = **0xFFFF**

Integer underflow

CYMOTIVE TECHNOLOGIES

Hell2CAP



Ask Me Anything

Lior.yaari@cymotive.com

Website

Lior@imperium-sec.com

LinkedIn

Twitter: @lior_yaari

CYMOTIVE TECHNOLOGIES

DEEPSEC