Trustwave®
SpiderLabs®

Hacking the Fast Lane: security issues in 802.11p, DSRC and WAVE

Bruno Gonçalves de Oliveira
boliveira@trustwave.com
Rob Havelt
rhavelt@trustwave.com

Trustwave®
SpiderLabs®

THIS IS NOT A "USER-MODE CALLBACK TO RING0" PRESENTATION

Agenda

- **Acronyms**
- **Overview**
- **Supposed to do**
- **Protocol Stack**
- **WAVE**
  - What is defined by IEEE
- **Attacks Scenarios**

whoami

BIO

- **SpiderLabs:~ Trustwave$ whois BrunoGO**
  - Computer Engineer;
  - Security certs,
  - Security Consultant at Trustwave's Spiderlabs in the Network Penetration Testing Team
  - 9+ years on information security field;
  - Previously talk at SOURCE Barcelona 2010 (Spain), DEF CON 18 (USA), HITBSec Conf 2009 (Malaysia), ToorCon X (USA), YSTS 2.0/3.0, H2HC IV/VI (Brazil), among others.
  - Just accepted for BlackHat DC.

What are ALL these acronyms?

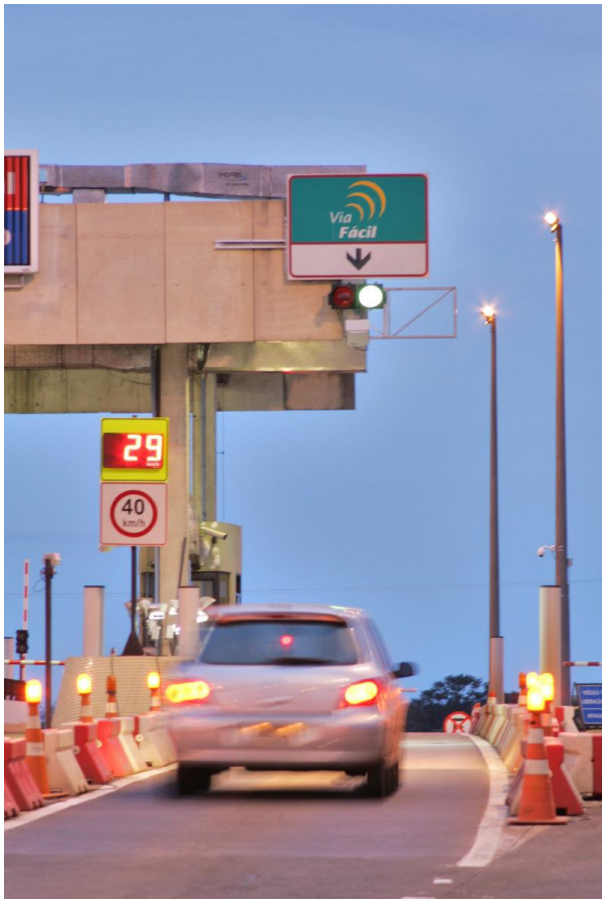
- **WAVE (Wireless Access in Vehicular Environments**
  - Mode used by 802.11 devices to run in the DSRC band
- **DSRC (Dedicated Short Range Communications)**
  - Name of 5.9Ghz band
- **IEEE 802.11p**
  - Based on ASTM Standard E2213-03

Overview

		Wireless Technology												
		5.9 GHz DSRC	2.5-3G PCS and Digital Cellular	Bluetooth	Digital Television(DTV)	High Altitude Platforms	IEEE 802.11 Wireless LAN	Nationwide Differential Global Positioning System	Radar	Remote Keyless Entry (RKE)	Satellite Digital Audio Radio Systems (SDARS)	Terrestrial Digital Radio	Two-Way Satellite	Ultrawideband (UWB)
Capabilities	Range	1000 m	~4-6 km	10 m	~40 km	120 km	1000 m	300-400 km	2 km	30 m	US 48 States	30-50 km	N/A	15-30 m
	One-Way To Vehicle	X			X	?		X	X	X	X	X		?
	One-Way From Vehicle	X				?			X					?
	Two-Way	X				?							X	?
	Pont-To-Point	X	X	X		?	X			X			X	?
	Point-To-Multipoint	X	X	X	X	?	x	X	X		X	X		?
	Latency	200 µsec	1.5-3.5 sec	3-4 Sec	10-30 sec	?	3-5 sec	N/A	N/A	N/A	10-20 sec	10-20 sec	60+sec	?

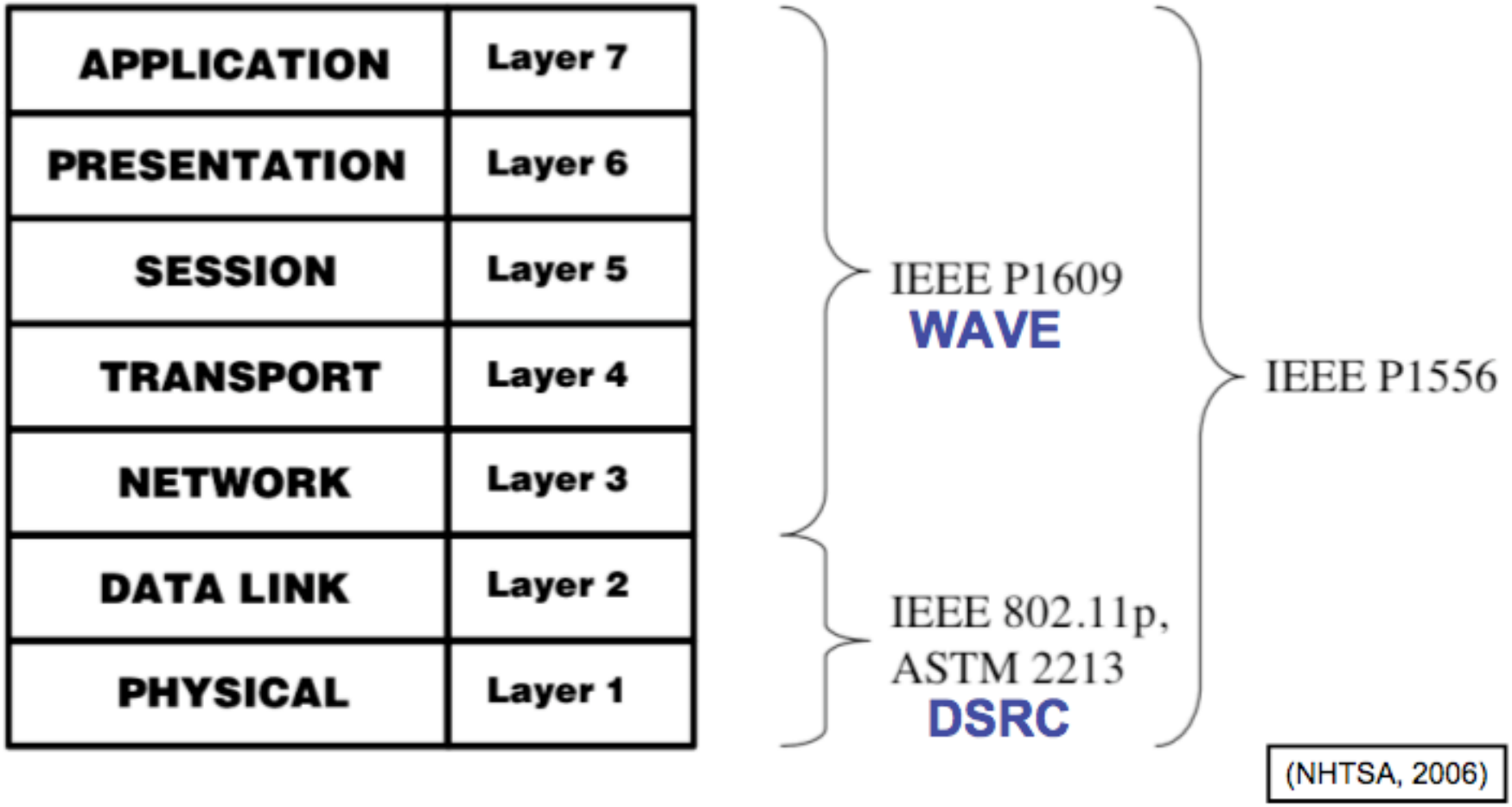
What it is purposed (mainly)

Electronic Tolls



Emergency Vehicles

Protocol Stack



WAVE – Wireless Access in Vehicular Environments

- **Defined by IEEE 1609.0-4**
  - Architecture
  - Resource Manager
  - Security Services for App
  - Networking Services
  - Multi-Channel Operations

Trustwave®
SpiderLabs®

Architecture

WAVE – Wireless Access in Vehicular Environments - Architecture

RSU – Road Side Unit

A wireless access in vehicular environments (WAVE) device that operates only when stationary and supports information exchange with onboard units (OBUs).

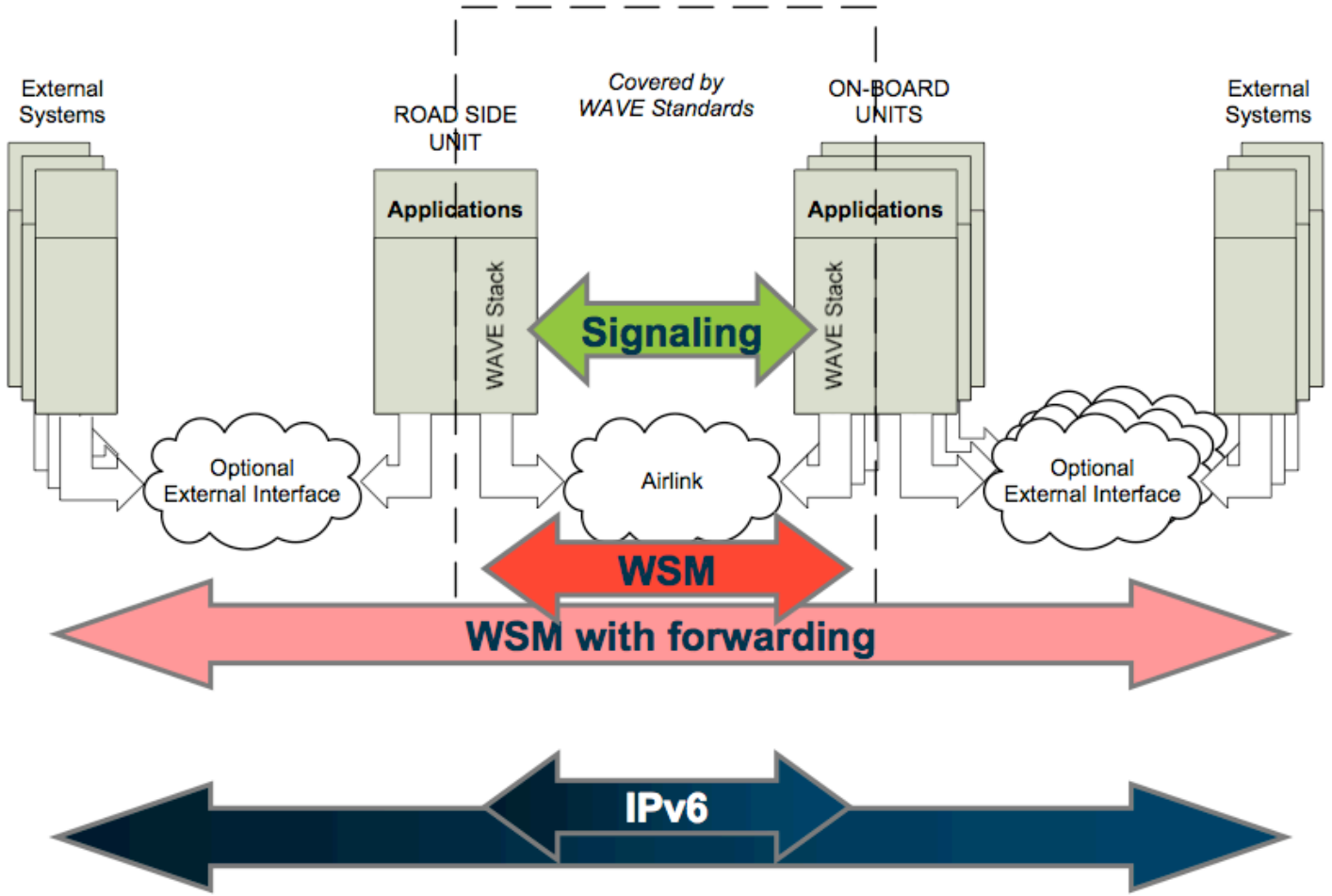
OBU – Onboard Unit

A wireless access in vehicular environments (WAVE) device that can operate when in motion and supports information exchange with roadside units (RSUs) and other OBUs.

WAVE – Wireless Access in Vehicular Environments - Architecture

Onboard Unit (OBU) – DSRC Device

WAVE – Wireless Access in Vehicular Environments - Architecture



Trustwave®

SpiderLabs®

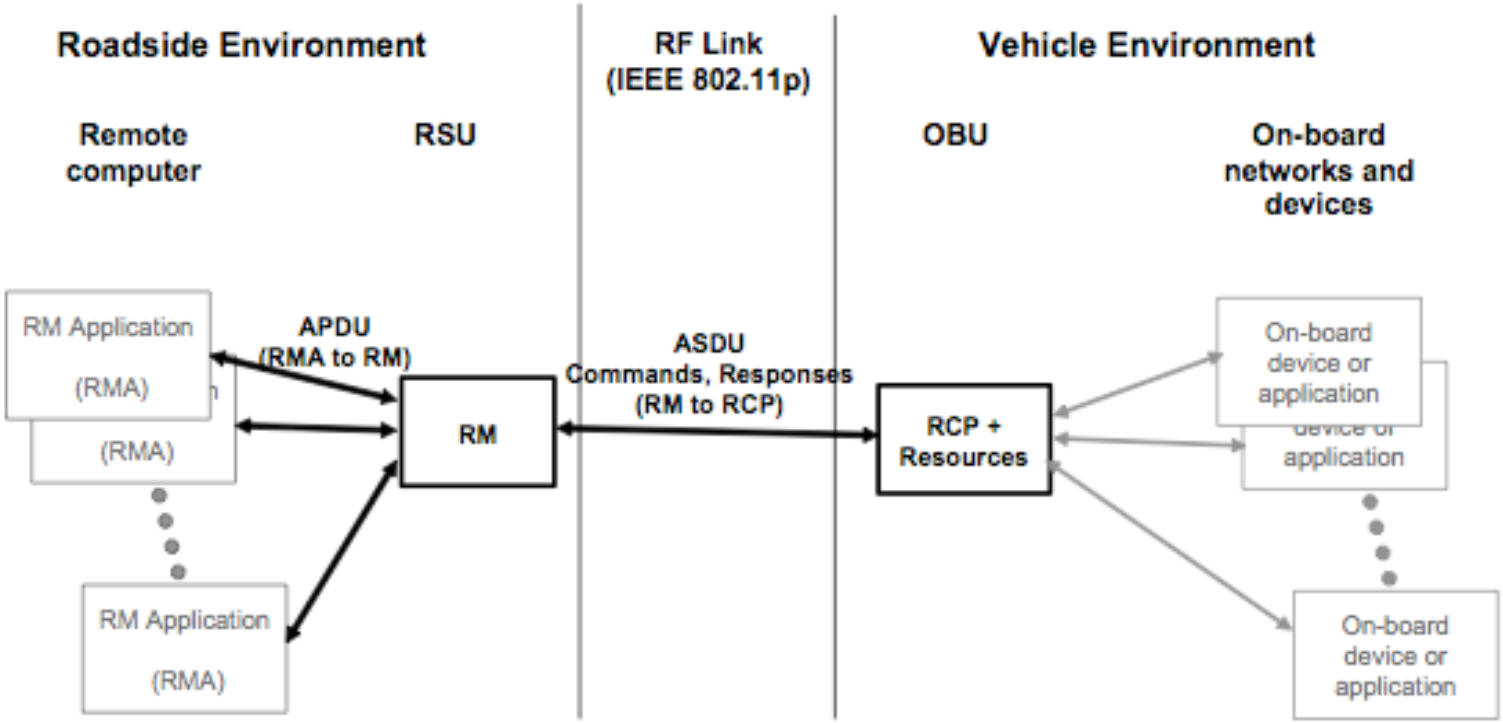
Resource Manager

WAVE – Wireless Access in Vehicular Environments – Resource Manager

The external interfaces:

- Resource Manager Application (RMA)
- Resource Manager (RM)
- Resource Command Processor (RCP)

WAVE – Wireless Access in Vehicular Environments – Resource Manager



Trustwave®

SpiderLabs®

Channel

WAVE – Wireless Access in Vehicular Environments - Channel

Channel Allocation for WAVE

- Seven 10 Mhz Channels

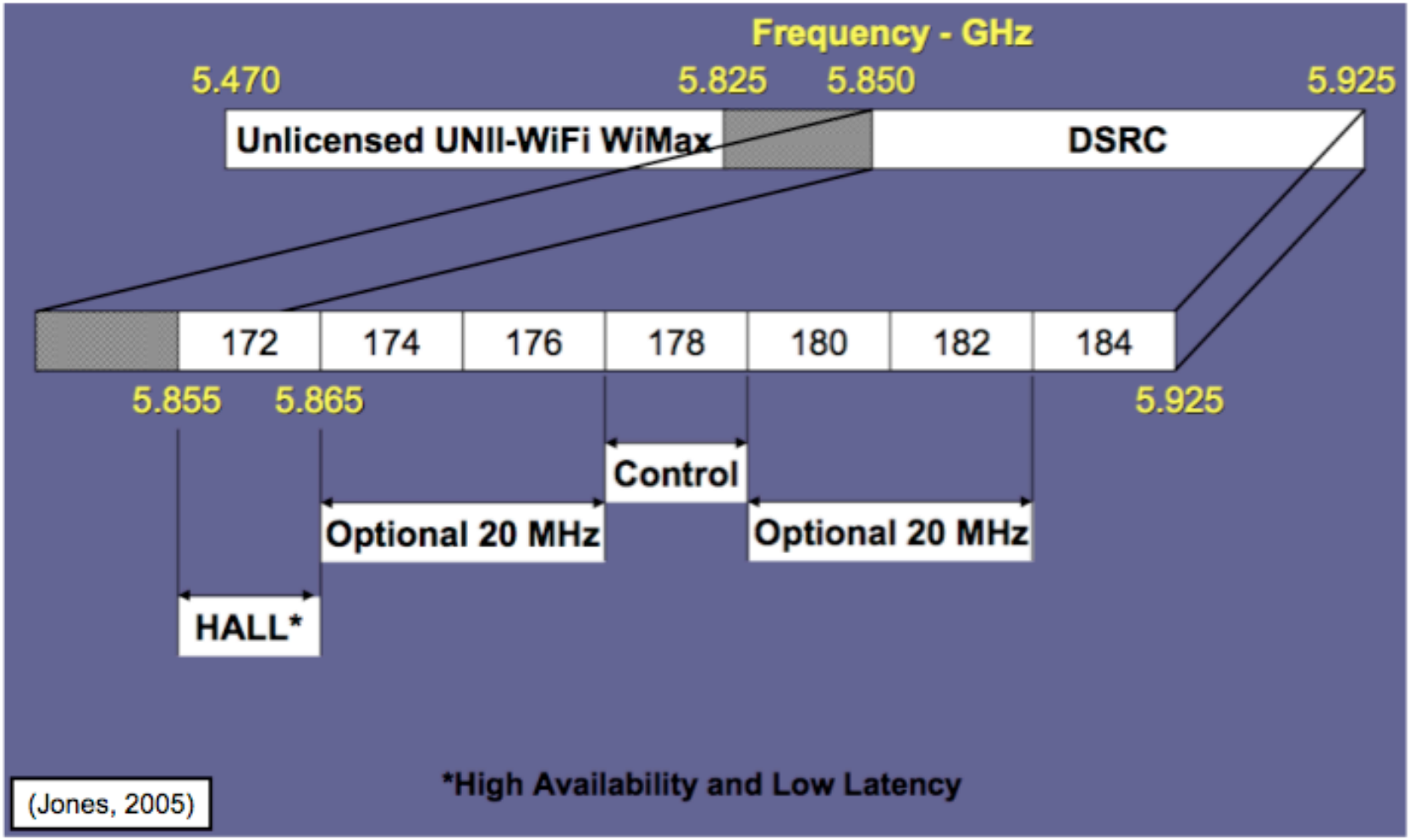
Data Rates for WAVE (Mbits)

- 3, 4.5, 6, 9, 12, 18, 24, 27

Modulations

- BPSK OFDM, QPSK OFDM, 16-QAM OFDM, 64-QAM OFDM

WAVE – Wireless Access in Vehicular Environments - Channel



WAVE – Wireless Access in Vehicular Environments - Channel

Setting-up WAVE Mode:

- Channel scan disabled
- Channel 178
- 6 Mbps data rate
- Receives any mandatory data rate

Trustwave®

SpiderLabs®

Network

WAVE – Wireless Access in Vehicular Environments - Network

Can work in 2 ways

- WAVE Short Message Protocol (WSMP)
- IPv6

WAVE – Wireless Access in Vehicular Environments - Network

WAVE Short Message Protocol (WSMP)

WSM-WaveShortMessage.request
(
ChannelInfo,
WsmVersion,
SecurityType,
ProviderServiceIdentifier,
TransmissionPriority,
Length,
Data,
Peer MAC address
)

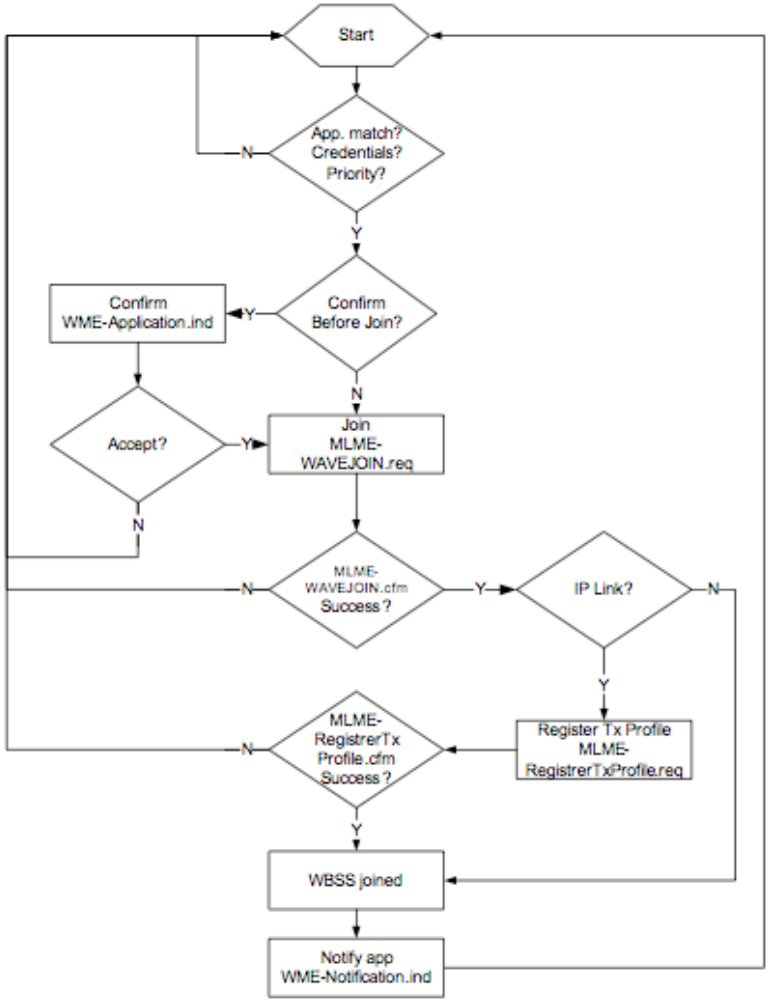
WAVE – Wireless Access in Vehicular Environments - Network

WAVE Basic Service Set (WBSS)

A set of two or more WAVE devices participating in communications among each other on a SCH. A WBSS is initiated by a WAVE device using a WAVE Announcement action frame on the CCH.

It's used like an access-point!

WAVE – Wireless Access in Vehicular Environments - Network



Trustwave®

SpiderLabs®

Security

WAVE – Wireless Access in Vehicular Environments - Security

- **Authenticate messages (certificate issued by the vendor)**
- **Encrypt confidential data**
- **Messages must be short and transactions fast**

Trustwave®
SpiderLabs®

Attacks Scenarios

Attacks Scenarios

Impersonate

- It's not identified by MAC (or any hw specification)
- Use the same certificate (should worth a test)

DoS

- When systems are working on WSMP, waiting short messages.

Physical Attacks

- Tracking Information (parking systems - cheats)

Attack Scenarios

Eavesdropping

- What is unencrypted ?
  - Any message **CAN** be unencrypted

- *JUST* the data field is encrypted, the packet is still available

Attack Scenarios - Eavesdropping

How?

- USRP (Universal Software Radio Peripheral) (http://www.ettus.com)

- GNU Radio (Framework for creation of software defined radios)

- Maybe something on BH DC ;)

That's it! Thanks!

No questions please! ;)

boliveira@trustwave.com

@mphx2