BUSINESS-e
BE Your Security

CAR HACKING: the evolution of existing solutions and the emerging standards and tools

Milano – 14° Workshop di Automotive SPIN
10/11/2016

BUSINESS-e

BE Your Security

Business-e Spa è una società del Gruppo Itway, Leader da 20 anni nel settore della sicurezza informatica.

Grazie a partnership strategiche con i migliori vendor del settore, forniamo consulenza e servizi sulla sicurezza di reti, sistemi, applicazioni e contenuti (back-up e recovery), sulla gestione dell'identità degli utenti e degli accessi, sulla protezione dei dati e delle Informazioni e sull'ottimizzazione dei data center e delle infrastrutture di rete.

Un aspetto chiave della nostra strategia, ed elemento di forte differenziazione sul mercato, sono i Cyber Security Managed Services erogati tramite SOC localizzati in Italia con personale italiano certificato, per i quali dal 2014 siamo l'unica azienda italiana citata da GARTNER nel Magic Quadrant Report dei Managed Security Services Provider.

Iso 9001:2008 Certified

Iso 27001:2013 Certified

Business-e S.p.A.

An Itway Company Group

1. Azienda multinazionale, a capitale italiano e quotata in Borsa
2. Leader da 20 anni nel settore della Cyber Security
3. Dal 2014 unica azienda italiana citata da Gartner nel Magic Quadrant degli MSSP
4. SOC configurato in Disaster Recovery e certificata ISO:SEC 27001
5. Azienda più volte certificata NATO per lavorare in tema Cyber Security su ambienti militari classificati
6. BU specifiche sulla sicurezza informatica:
    - Infrastructure Security,
    - Security Consulting (comprende un team di Ethical Hacker)
    - MSS (Servizi di Sicurezza Gestiti)
7. Organizzazione commerciale per mercati (Industry, Finance, PA, Telco) che ci permette di conoscere in maniera verticale e specifica tutte le esigenze di security
8. Strutture di prevendita dedicate per vertical d'offerta a supporto della struttura di vendita
9. Conoscenza a 360°delle tecnologie dei principali vendor di security
10. Continuo scouting sul mercato di nuove tematiche e nuove soluzioni per la Cyber Security

FATTURATO

120 milioni

PROFESSIONISTI

Oltre 300

CERTIFICAZIONI

Oltre 700

SEDI

18

Di cosa Parleremo?

1. Chi è Business-e
2. Le attuali metodologie di Ethical Hacking
3. Estendere le metodologie esistenti al mondo automotive
4. Car Hacking – un esempio di reverse engineering
5. Conclusioni

BUSINESS-e
BE Your Security

Le attuali metodologie di Ethical Hacking

Milano – 14° Workshop di Automotive SPIN
10/11/2016

Penetration Test

Fase 1 Pre-Assessment

Step 1: Preparazione ambiente di test

- Gestione problematiche legali (Liberatorie, NDA, perimetro)
- Definizione ambiente di lavoro (onsite, VPN, …)
- Intervista, Informazioni e Produzione **Piano di Verifica**

Fase Operativa

Step 2: Vulnerability Assessment

- Analisi automatica di Ip e Web Application
- Ricerca Vulnerabilità, Configurazioni errate, Errori di sviluppo secondo la metodologia OSSTMM
- Approccio manuale per confermare falsi positivi/negativi

Step 3: Sfruttamento delle Vulnerabilità

- Attuazione realistica di scenari di attacco
- Analisi dei risultati e applicazione delle ultime tecniche di attacco per **simulare cosa potrebbe fare un attaccante sui sistemi**

Fase 2 Reportistica

Step 4: Produzione di una Reportistica ad hoc

- Produzione di **un Executive Summary** per il Management basato su standard ISO 27001
- **Allegati Tecnici** con il dettaglio degli attacchi
- **Contromisure a vario livello** per il rientro

Code Review

Fase 1 Pre-Assessment

Step 1: Richiesta Informazioni

- Gestione problematiche legali (Liberatorie, NDA, perimetro)
- Richiesta documentazione di progetto/sviluppo
- Informazioni sul codice

Fase Operativa

Step 2a: Decompilazione o analisi binari

- Analisi di programmi di terze parti o analisi “low level” su binari compilati
- Individuazione informazioni e analisi organizzazione e problematiche principali

Step 2b: Analisi del codice

- Uso di tool automatici per individuare le vulnerabilità
- Approccio manuale per confermare le problematiche
- Analisi teorica e valutazione dei falsi positivi

Fase 2 Reportistica

Step 3: Produzione di una Reportistica ad hoc

- Produzione di un **Executive Summary** per il Management
- **Allegati Tecnici** con il dettaglio delle problematiche e l’analisi teorica
- **Contromisure a vario livello** per il rientro

Vulnerability Assessment

Fase 1
Pre-Assessment

Step 1: Preparazione ambiente di test

- Gestione problematiche legali (Liberatorie, NDA, perimetro)

Fase Operativa

Step 2: Vulnerability Assessment

- Analisi automatica di Ip e Web Application

Step 3: Identificazione delle Vulnerabilità

- Analisi dei report dei tool automatici
- Categorizzazione delle vulnerabilità - Rischio, Impatto

Fase 2
Reportistica

Step 4: Produzione di una Reportistica ad hoc

- Produzione di un Executive Summary
- Contromisure per i rientri

Web Application Security

Fase 1 Pre-Assessment

Step 1: Preparazione ambiente di test

- Gestione problematiche legali (Liberatorie, NDA, perimetro)
- Definizione ambiente di lavoro e Analisi Architettura
- Intervista, Informazioni e Produzione **Piano di Verifica**

Fase Operativa

Step 2: Web Vulnerability Assessment

- Ricerca Vulnerabilità, Configurazioni errate, Errori di sviluppo specifiche per le Web Application
- Applicazione delle metodologie OWASP per l'analisi

Step 3: Sfruttamento delle Vulnerabilità

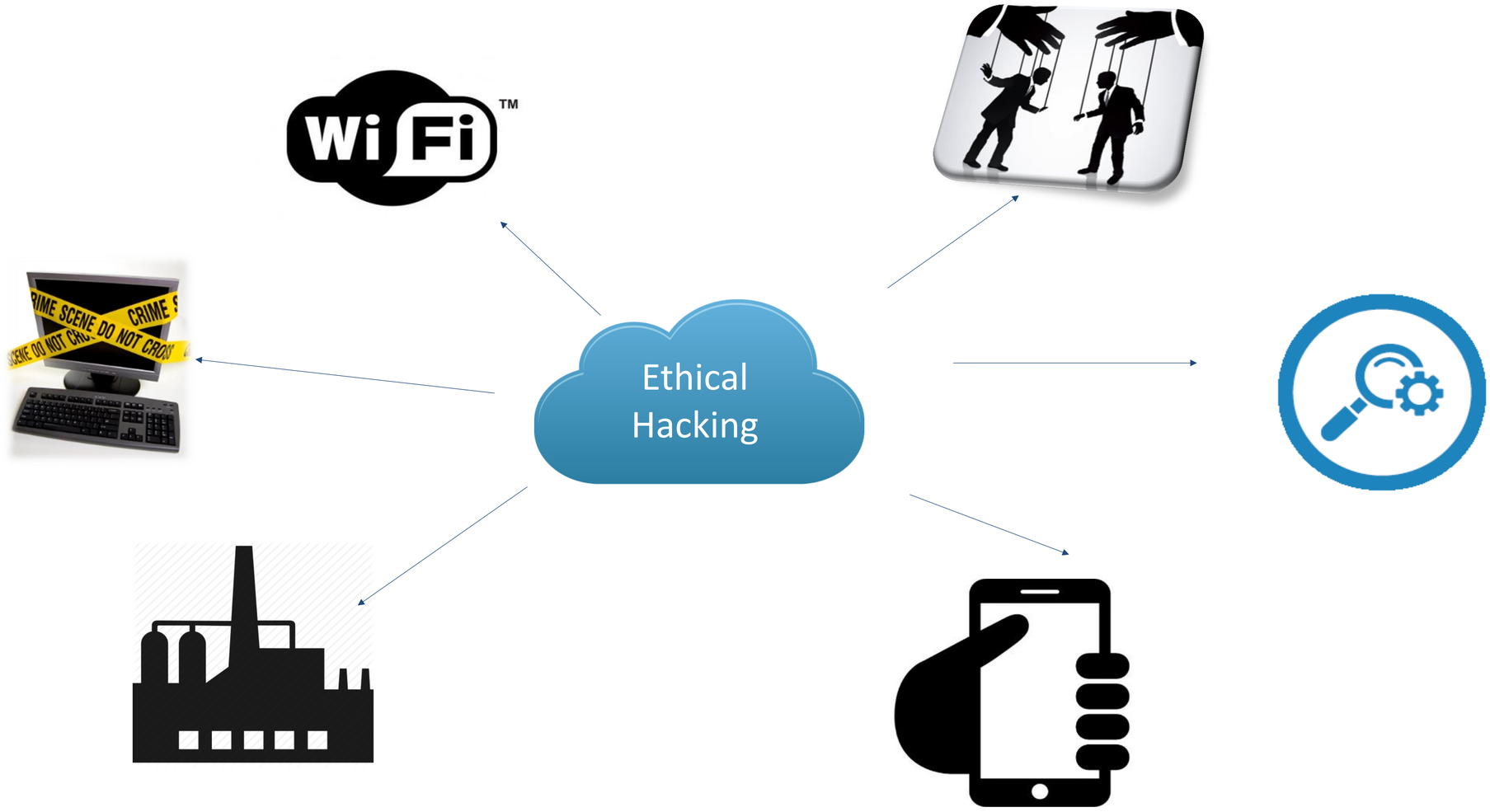
- Sfruttamento delle vulnerabilità su **Web Application** custom (SQL Injection, XSS, Cross Site Request Forgery, …)
- Analisi degli scenari di attacco Web 2.0, attuabili tramite Social Network, mail, spam, …

Fase 2 Reportistica

Step 4: Produzione di una Reportistica ad hoc

- Produzione di un **Executive Summary** per il Management basato su standard ISO 27001
- **Allegati Tecnici** con il dettaglio degli attacchi
- **Contromisure a vario livello** per il rientro

Attività di Ethical Hacking



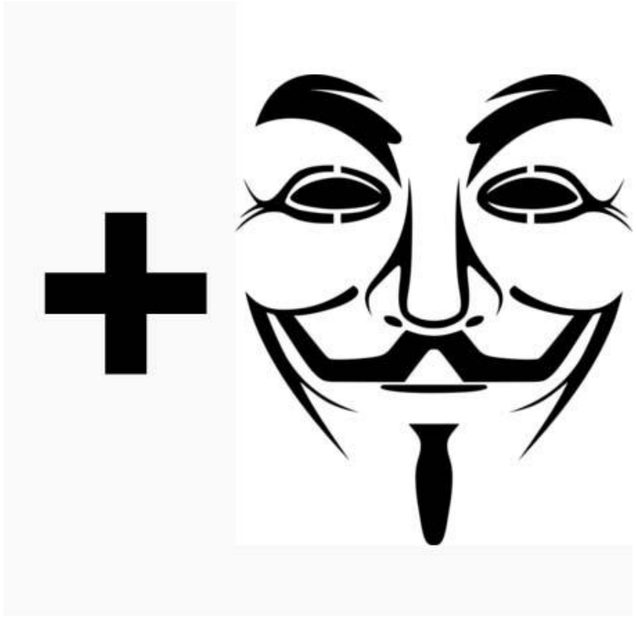
BUSINESS-e
BE Your Security

Car Hacking
un esempio di Reverse Engineering

Milano – 14° Workshop di Automotive SPIN
10/11/2016

CAR HACKING

Cosa è il Car Hacking? Un esempio di reverse engineering



BUSINESS-e
BE Your Security

COSA E' POSSIBILE FARE?

SENSORI

Controllare i sensori dell'automobile: pressione, umidità, velocità, RPM, ABS, airbag, …

ATTUATORI

Controllare i finestrini, aria condizionata, freni, fari, …

MOTORE

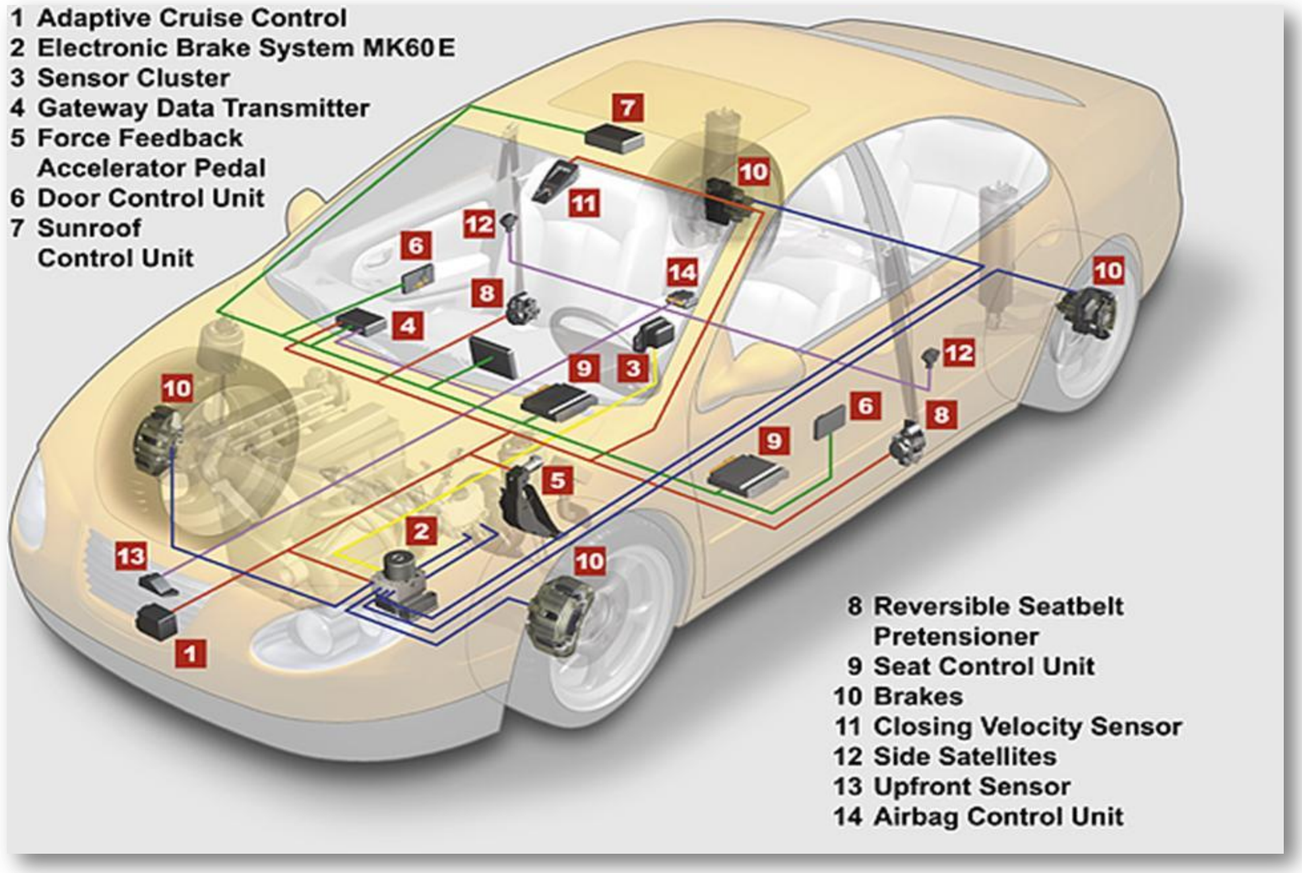
Accensione, spegnimento, afflusso benzina, accelerazione, coppia, …

MULTIMEDIA

Radio, CD, computer di bordo, navigatore, …

COSA è POSSIBILE FARE?

Dipende da quali funzionalità ha l'automobile



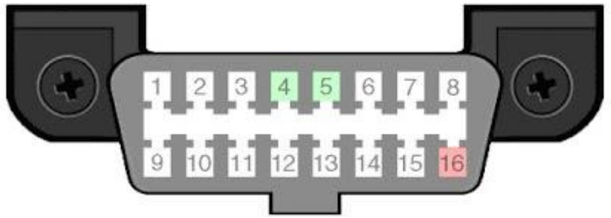
POTENZIALI RISCHI…

- Spegnere i fari di notte
- Spegnere il motore in autostrada
- Accelerare ad un incrocio
- Girare lo sterzo in velocità
- Chiudere/aprire portiere

NOZIONI DI BASE

La revisione dell'automobile

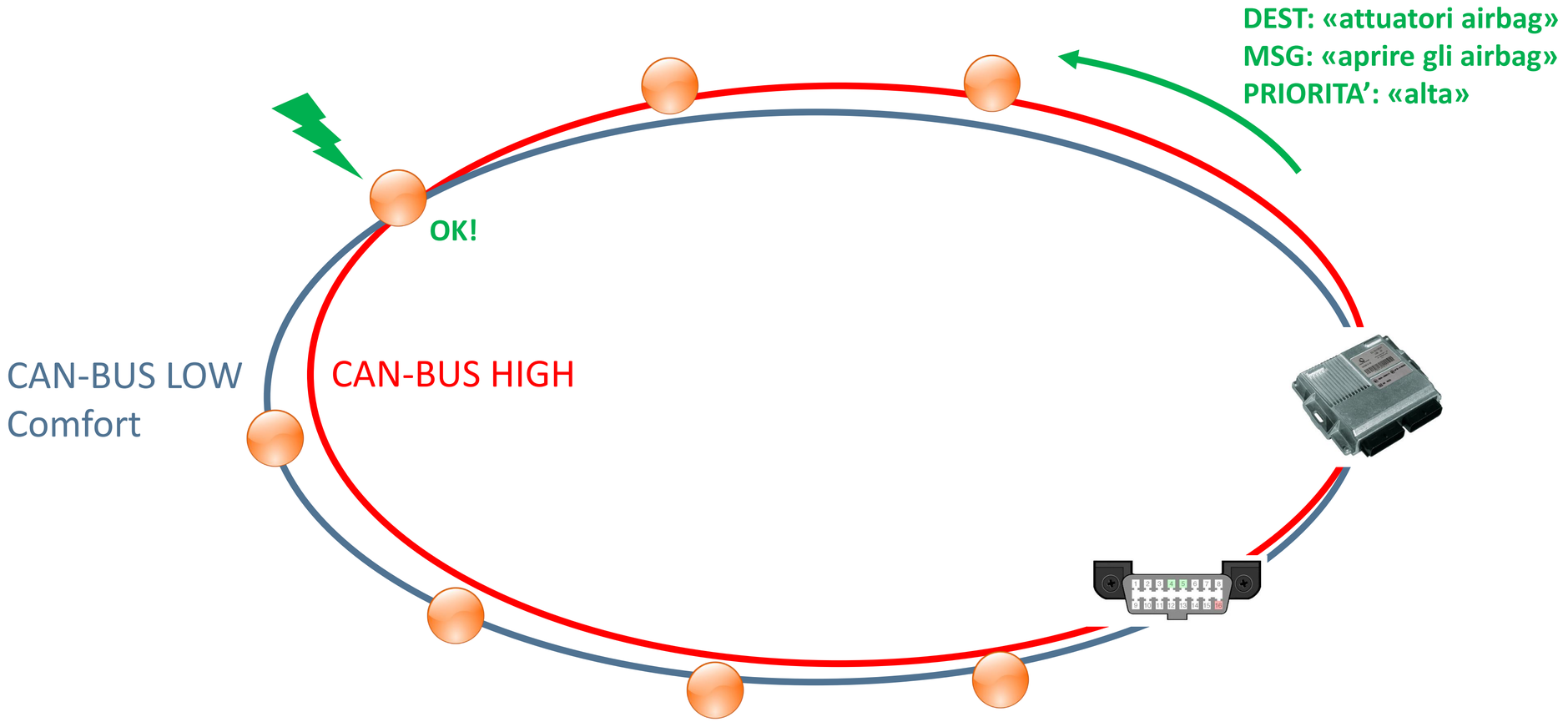
- Il dispositivo si collega alla centralina
- Connettore OBDII entro 60 cm dal volante



1 Make/Model Specific
2 SAE J1850-PWM POS(+) or SAE J1850-VPW POS(+)
3 Make/Model Specific
4 Chassis Ground (all protocols)
5 Signal Ground (all protocols)
6 ISO15765-4 CAN-Bus High
7 ISO9141-2 K-Line or ISO14230-4 KWP2000 K-Line
8 Make/Model Specific
9 Make/Model Specific
10 SAE J1850-PWM NEG(-)
11 Make/Model Specific
12 Make/Model Specific
13 Make/Model Specific
14 ISO15765-4 CAN-Bus Low
15 ISO9141-2 L-Line or ISO14230-4 KWP2000 L-Line
16 +12v (always on) (all protocols)

LA RETE VEICOLARE

Il CAN-BUS



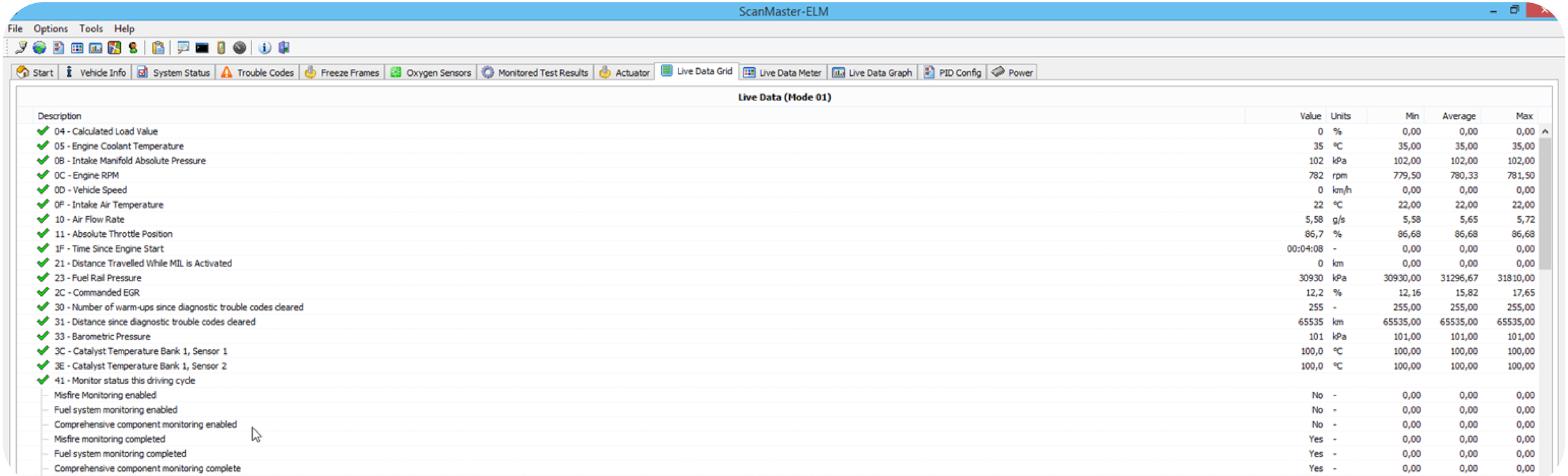
COSA SERVE

OBD-II adapter

- Economico ed acquistabile su internet
- WiFi, Bluetooth, USB cable
- La versione WiFi crea un hotspot
- Controllabile da PC o smartphone

SPERIMENTAZIONE

Ford Fiesta 2011



Description	Value	Units	Min	Average	Max
04 - Calculated Load Value	0	%	0,00	0,00	0,00
05 - Engine Coolant Temperature	35	°C	35,00	35,00	35,00
0B - Intake Manifold Absolute Pressure	102	kPa	102,00	102,00	102,00
0C - Engine RPM	782	rpm	779,50	780,33	781,50
0D - Vehicle Speed	0	km/h	0,00	0,00	0,00
0F - Intake Air Temperature	22	°C	22,00	22,00	22,00
10 - Air Flow Rate	5,58	g/s	5,58	5,65	5,72
11 - Absolute Throttle Position	86,7	%	86,68	86,68	86,68
1F - Time Since Engine Start	00:04:08	-	0,00	0,00	0,00
21 - Distance Travelled While MIL is Activated	0	km	0,00	0,00	0,00
23 - Fuel Rail Pressure	30930	kPa	30930,00	31296,67	31810,00
2C - Commanded EGR	12,2	%	12,16	15,82	17,65
30 - Number of warm-ups since diagnostic trouble codes cleared	255	-	255,00	255,00	255,00
31 - Distance since diagnostic trouble codes cleared	65535	km	65535,00	65535,00	65535,00
33 - Barometric Pressure	101	kPa	101,00	101,00	101,00
3C - Catalyst Temperature Bank 1, Sensor 1	100,0	°C	100,00	100,00	100,00
3E - Catalyst Temperature Bank 1, Sensor 2	100,0	°C	100,00	100,00	100,00
41 - Monitor status this driving cycle					
Misfire Monitoring enabled	No	-	0,00	0,00	0,00
Fuel system monitoring enabled	No	-	0,00	0,00	0,00
Comprehensive component monitoring enabled	No	-	0,00	0,00	0,00
Misfire monitoring completed	Yes	-	0,00	0,00	0,00
Fuel system monitoring completed	Yes	-	0,00	0,00	0,00
Comprehensive component monitoring complete	Yes	-	0,00	0,00	0,00
Catalyst monitoring enabled	No	-	0,00	0,00	0,00

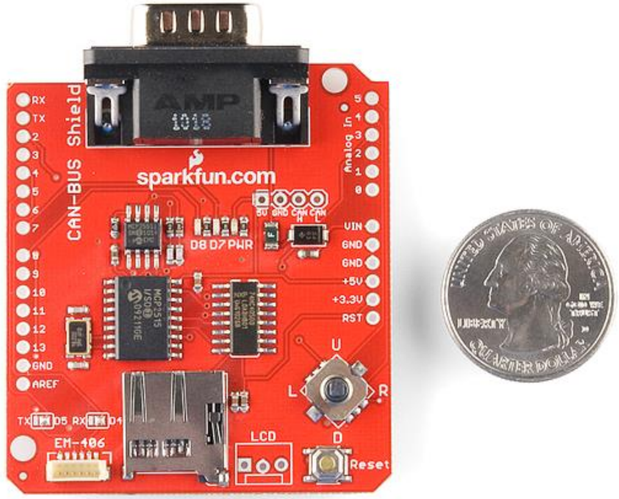
SPERIMENTAZIONE

Ford Fiesta 2011

COSA SERVE

Better OBD-II adapter – in scrittura

- Shield per Arduino
- Cavo di collegamento
- Connesso al PC tramite USB (o GSM ☺)



REVERSE ENGINEERING

Ford Fiesta 2011

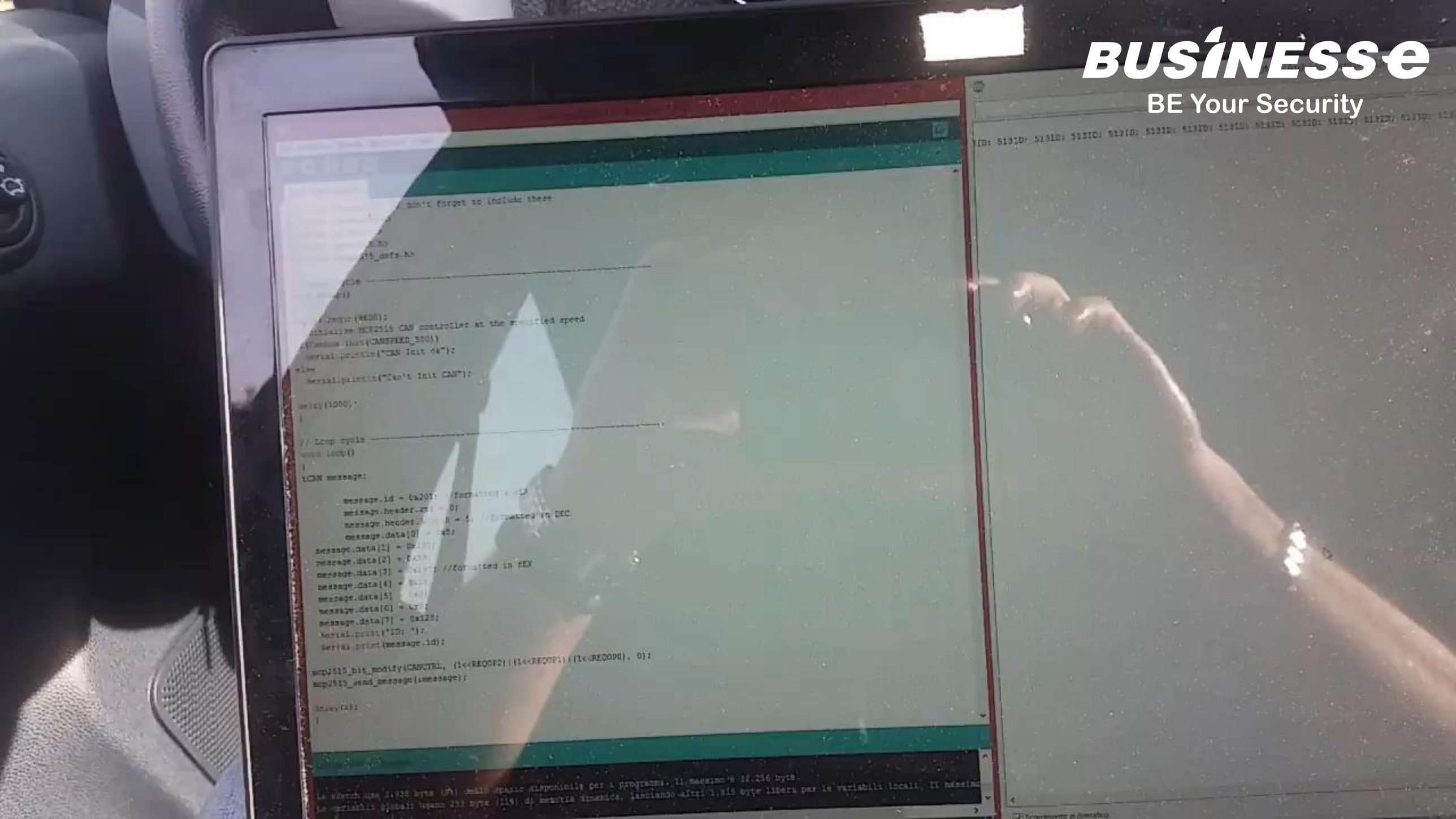
Come?

- Ford Fiesta 2011 ha una centralina **ELM327 1.4b**
  - Supporta comandi AT (Hayes commands)

- OBD-II WiFi
- nmap –sS –n –PN –vvvv 192.168.0.0/24
- Port 80, 35000

- Telnet 192.168.0.10 35000
  - ATI
  - ATL1
  - ATH1
  - ATS1
  - ATAL
  - ATSP0
  - ATMA

```
Telnet 192.168.0.10

201 03 0B 3F B2
205 21 FC 01 FC 02 5A 01 FC
20F 75 42 27 10 00 00 00 00
211 FF FE 81 FF 48 48 0
BUFFER FULL

>
240 01 00
073 1C 21 16 E9 17 83 14 CE
090 C7 08 F7 07 C7 8A 17 D9
190 00 53 00 00 00 0B 00 00
20E 27 10 BC 0C 80 00 00 00
20F 75 42 27 10 00 00 00 00
201 03 06 3F 7F
211 FF FE 81 FF 48 48 00 0C
200 27 03 27 08 27 08 80 00
205 2
BUFFER FULL

>

240 01 00
080 26 F6 02 A2 00 10 34 00
073 1C 21 16 E9 17 83 14 CE
090 27 08 F7 09 C7 83 17 D9
20E 27 10 1C AC 80 00 00 00
200 27 02 27 03 27 03 80 00
201 03 0E 3F E6
205 21 FC 01 FC 02 5A 01 FC
20F 75 42 27 10 00 00 00 00
211 FF FE 81 FF 48 48 00 22
BUFFER FULL

>

4B0 27 10 27 10 27 10 27 10
080 26 F6 02 A2 00 10 46 00
460 03 81 00 00
433 00 01 32 01 00 A2 87 00
073 1C 21 16 E9 17 83 14 CE
090 C7 08 F7 08 C7 82 17 D9
20E 27 10 BC 0C 80 00 00 00
20F 75 42 27 10 00 00 00 00
201 03 0A 40 33
211 FF FE 81 FF 48
BUFFER FULL

>
```


BUSINESSe
BE Your Security

PROBLEMATICHE DI SICUREZZA

1

VULNERABILE “BY DESIGN”
Traffico in chiaro – Messaggi in broadcast – Il mittente non ha bisogno di conoscere come verrà processato il messaggio

CONNETTORE OBD-II DI SERIE
Introdotto da diversi produttori di serie sui modelli più recenti

2

CONCLUSIONI

Progettato come una rete isolata

Come nel caso dei sistemi Scada/ICS

Comunicazione con rete internet

Problematiche di sicurezza (cd. Stuxnet)

Necessità di comprendere i punti deboli del sistema

E le migliori contromisure da adottare per garantire una integrazione sicura

Il successo di una nuova tecnologia

Il livello di sicurezza può influenzare il successo o meno di una tecnologia

Grazie

Fabrizio De Santis

fabrizio.desantis@business-e.it

www.business-e.it

AN ITWAY GROUP COMPANY

ITALY, FRANCE, SPAIN, PORTUGAL, GREECE, TURKEY, U.A.E.
Ravenna, Milano, Trento, Massa, Roma, Bari, Paris, Barcelona,
Madrid, Lisboa, Athina, Istanbul, Ankara, Dubai-Hamiryah-Sharja