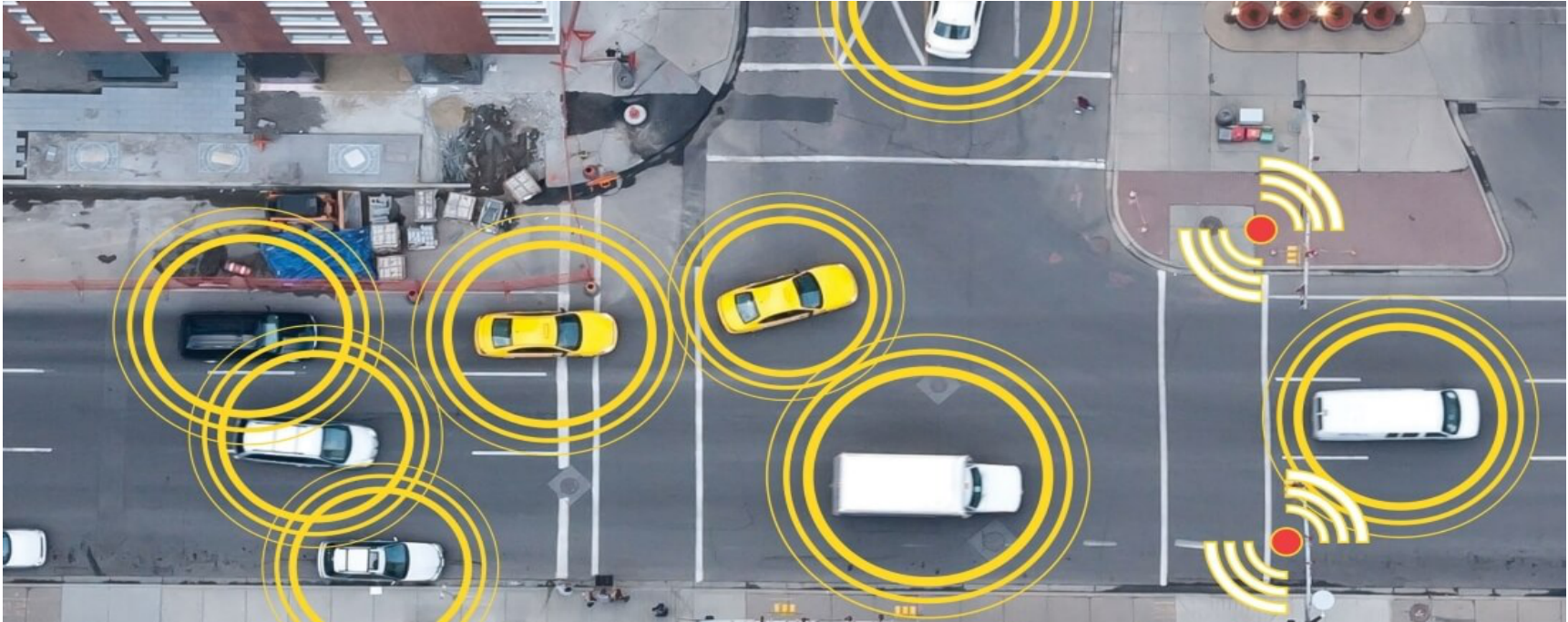


L'auto connessa: una pessima idea



Alessandro Guarino
StudioAG - DFA

e-Privacy XX Autumn - *Roma* 5/11/2016
Sala del Carroccio

Introduzione

Nonostante i possibili vantaggi, connettere ad Internet in permanenza un'automobile non è una buona idea....

Protezione dei dati e privacy: Avete mai dato il consenso per il trattamento dei dati alla vostra automobile?

(Eppure, i veicoli moderni sono uno dei “raccoglitori di dati” più impressionanti)

Cybersecurity: non esattamente tra i requisiti di progetto...



Alcune cifre

- Il numero di auto connesse (via app, smartphone, wireless integrati nei sistemi) passerà da 13,8 M nel 2013 a 82,6 M nel 2022 (IHS)

(quanto tempo prima che **tutti** i veicoli siano connessi?)

- "connected car systems will yield approximately \$14.5 billion in revenue from automotive data [...] by 2020."

Studio di IHS Automotive, 2013.



La posta in gioco...

Da dove verranno tutti questi soldi?

"Big Data assets found in the connected car—diagnostics, location, user experience/feature tracking, and adaptive driver assistance systems/autonomy..."

- IHS



Guerra sui dati

Winterkorn 2014 (al congresso della VDA):

"We seek connection to Google's data systems, but we still want to be the masters of our own cars,"

I dati (e i ricavi relativi) sono nostri (non di Google, ma nemmeno degli utenti).

Anche le case sono pienamente consapevoli del valore economico delle masse di dati.



Under the hood

Le auto moderne hanno a bordo ormai non una ma una pluralità di reti collegate tra loro, una mini-internet in movimento.

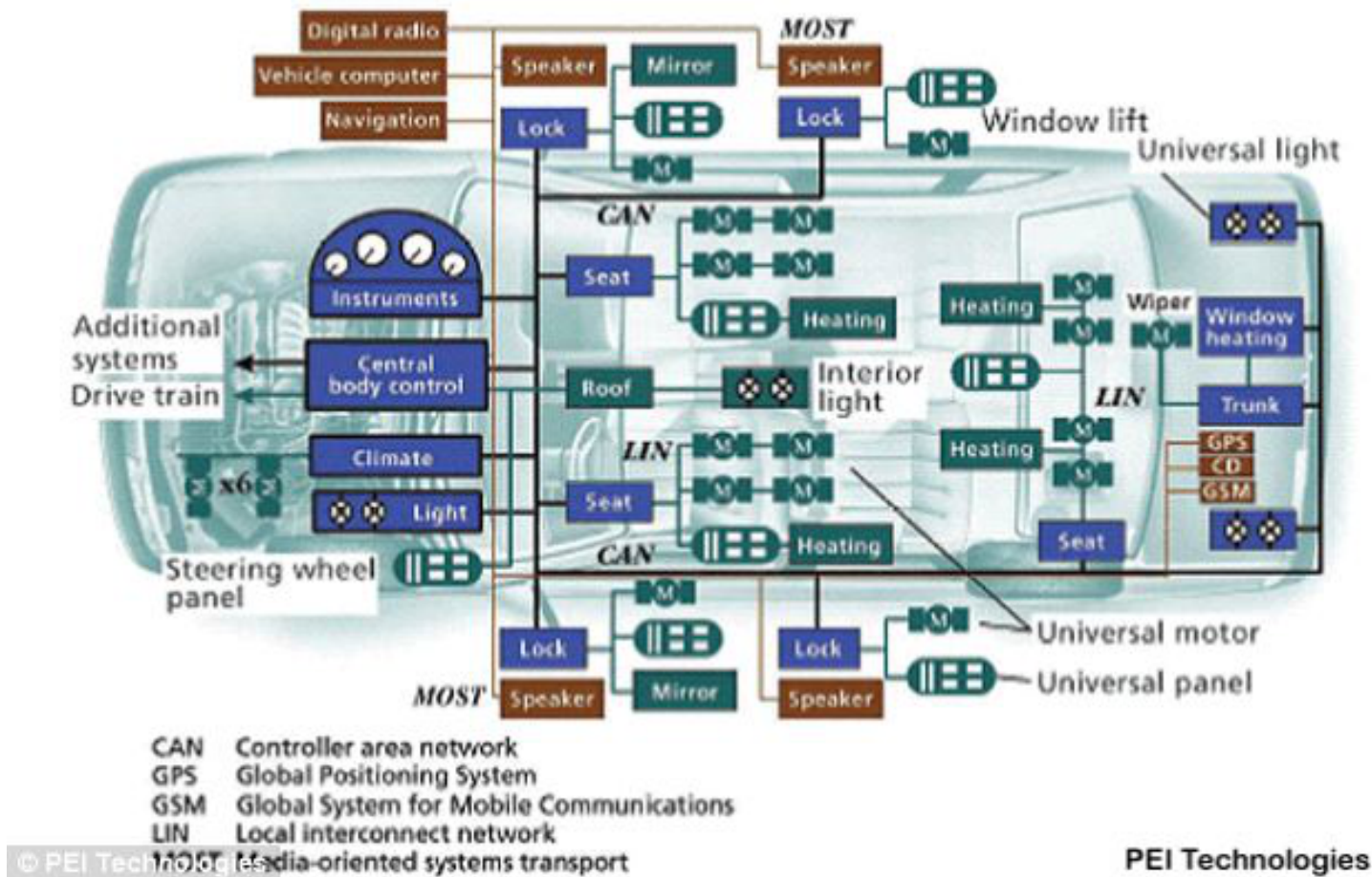
Connected vs. Autonomous – Le auto autonome non devono essere connesse a Internet per funzionare ma lo saranno.

Nota: molto di quello che si discute qui vale anche per i mezzi pesanti, le macchine agricole etc etc. , situazioni che presentano alcuni stakeholder e problematiche particolari.



Under the hood

CANbus: sensori, attuatori, elaboratori. Gli attuatori ormai possono controllare totalmente il veicolo – il gap con le auto autonome si assottiglia sempre più...



PEI Technologies



Under the hood – Futuro prossimo

OCTOBER 19

TSLA: 203.56 4.46 

Tesla announces all production cars now have fully self-driving hardware

Fred Lambert - 1 week ago  @FredericLambert

TESLA

TESLA MODEL 3

AUTOPILOT

SELF-DRIVING



Aperture

- La sicurezza della rete era tradizionalmente affidata all'isolamento fisico: unico punto di accesso l'interfaccia OBD, obbligatoria in Europe dal 2001 (come EOBD) e dal 2003 per le auto diesel.
- Ora esistono adattatori ODB-wireless con relative app
- Porte USB
- Wireless a corto raggio:
 - Bluetooth / Wifi / Radio e infrarossi
- Wireless a lungo raggio:
 - LTE 4G Modem



Cyber Safety

Ampia superficie di attacco

Attacchi via ODB necessitano dell'accesso fisico (all'interno) ma wireless no (basta essere vicini), meno ancora se la macchina è connessa a Internet in permanenza...

Alcune Criticità:

- Difficoltà di aggiornare i software
- Scarsa consapevolezza della sicurezza informativa e dei dati – connessione dei bus essenziali con quelli di intrattenimento



Cyber Safety

FCA Jeep Cherokee (1,4 milioni di veicoli richiamati nel 2015)

- Radio connessa a (entrambi) i bus CAN
- Uconnect (SO QNX) – collegato sia alle interfacce wifi e bluetooth sia ai sistemi critici



ANDY GREENBERG SECURITY 07.24.15 12:30 PM

**AFTER JEEP HACK, CHRYSLER
RECALLS 1.4M VEHICLES FOR
BUG FIX**



Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch.  ANDY GREENBERG/WIRED



Non solo sicurezza

Mitsubishi Outlander PHEV Hybrid

- AP Wifi. Password nel manuale... e fissa
- Il formato semplice del ssid permette di **geolocalizzare** tutte le auto (servizi di “*crowdsourced wardriving*” come wigle.net)
- Una volta penetrati sulla rete interna è stato possibile ricostruire il formato messaggi della app e... disabilitare l'antifurto (tra le altre cose)



Non solo sicurezza

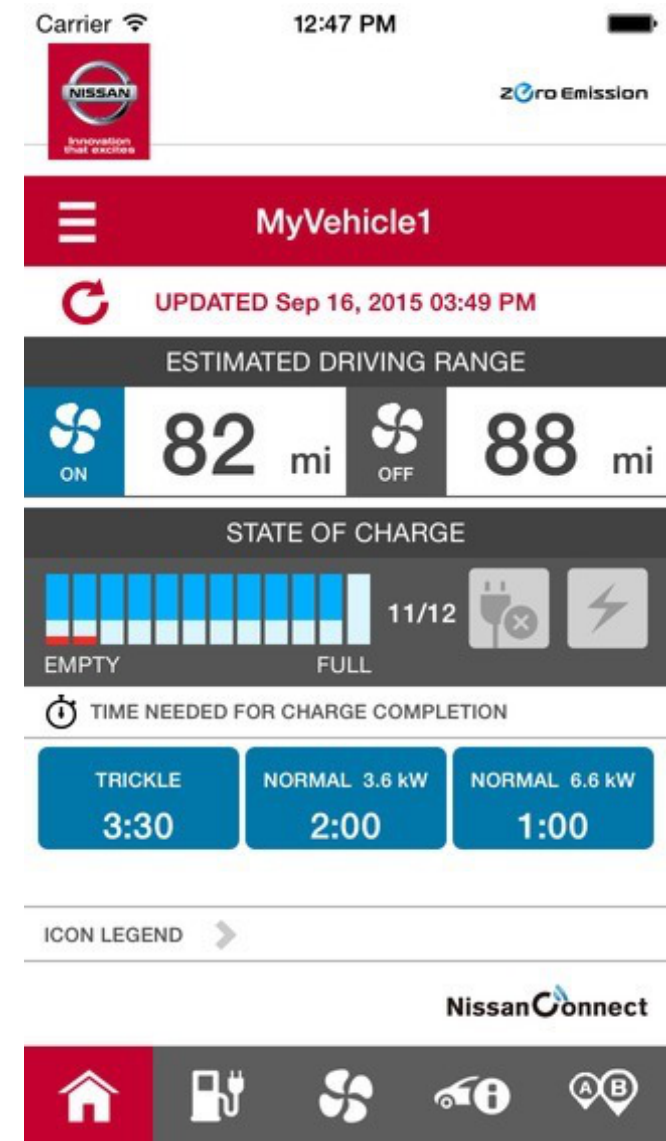
Nissan Leaf

– App “Nissan Connect”

Il numero di telaio(VIN) era

Sufficiente come autenticazione.

– E lo si può trovare...



(Big) Data

I dati grezzi: rpm, fasatura distribuzione, livello carburante, velocità istantanea, accelerazione, posizione (GPS), altitudine (GPS), temperatura acqua, carico motore, pressione carburante, pressione pneumatici (TPMS), potenza istantanea, temperature motore, posizione acceleratore, coppia, angolo di sterzo, pressione dei pneumatici, posizione del turbo...

I dati “dedotti”: consumi, velocità medie, violazioni (velocità + GPS), “stile di guida” (profilazione, simile al ritmo di battitura su tastiera)

Altri: celle “agganciate”, dash cam...



Controllo

Chi deve controllare l'uso di tutti questi dati?

Gli interessati sono molti.

I Principi della VDA (2014):

- Dati relativi all'auto (chilometraggio, velocità, etc): controllati dalla casa.
- Dati personali (indirizzo, consumi): controllati dal proprietario.
- I dati generati da infotainment e assistenza devono essere cancellabili da parte dell'utente.



Controllo

Le informative sono chiaramente insufficienti (se ci sono) e quasi sempre i servizi sono negati se si nega il consenso.

Difficile distinguere tra dati personali e dati relativi all'auto, date le possibilità attuali di profilazione individuale (big data e machine learning).



Dati personali?

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o **identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione**, ivi compreso un numero di identificazione personale;

1) «dato personale»:qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); **si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente,** con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;



Stakeholder 1/6

Gli attori interessati a questi dati sono molti:

- Proprietario, guidatore (possono non coincidere, anche in famiglia... Stesso problema dei telefoni “condivisi”)
- Casa produttrice
- Assicurazioni e periti
 - Premi legati allo stile di guida.
 - Stime dei danni, ricostruzione dei sinistri.



Stakeholder 2/6

- Compagnie di leasing (lo stile di guida influisce sul prezzo, come assicurazioni)
- Stato e Unione Europea
 - Fisco – Interessato all'intestatario e all'effettivo utilizzo: uso promiscuo (privato e professionale), uso privato di auto aziendali date come benefit etc etc
 - Altre amministrazioni pubbliche...
 - eCall. Quali dati verranno trasmessi? Quando? - in Italia eCall **E** Blackbox?



Stakeholder 3/6

- Polizia (stradale)
 - Ricostruzione degli incidenti
 - L'auto come “testimone” (anche contro il proprietario...). I dati sono visti come “obiettivi”, più affidabili delle testimonianze orali. Ex: GPS, ma accelerometri, rpm, velocità, sensori sui sedili (presenza di persone) e seggiolini, airbag, cinture allacciate...
 - Si può rifiutare l'accesso?



Stakeholder 4/6

- Vigili del fuoco, soccorritori, ospedali e strutture sanitarie
 - interessati al numero di feriti (sedili, seggiolini) e alla gravità (cinture sì no)
- Il sistema legale
 - Avvocati, Giudici, Consulenti Tecnici
- Fornitori/erogatori di servizi collegati all'automobile



Stakeholder 5/6

- Datori di lavoro (per le auto e i mezzi aziendali)
- Gestori delle flotte e delle “pool car”
- Assistenza stradale
 - interessati ai dati “raw”, OBD – devono avere accesso “in scrittura” ovviamente per la diagnostica e le riparazioni
 - trasmissione dati ad altri soggetti?
- Autonoleggi
- Car sharing



Stakeholder 6/6

- Taxi (dove esistono le compagnie di taxi ovviamente)
- Manutenzione e officine
 - di “marca” e indipendenti
 - integrazione con i dati personali della casa madre (storico manutenzione etc)
 - carrozzieri



Problemi aperti...

...per la privacy e la protezione dei dati

- classificazione, informativa, consenso
- necessità e proporzionalità
- dati che sembrano irrilevanti si prestano alla profilazione individuale
- dati personali (luoghi, itinerari, tempi e date, telefonate, playlist)
- difficile capire chi controlla quali dati
- retention e disposal



Problemi aperti...

...per la sicurezza (safety e security)

- preferire la comodità alla sicurezza nel caso delle automobili diventa pericoloso per l'incolumità fisica
- pressioni economiche per non includere la sicurezza sin dalla progettazione (security & safety by design)
- standard e regolazione (pochi standard o troppi)



Security – Soluzioni possibili

- Prevedere che ogni software possa fallire e incorporare sistemi di sicurezza hardware
- Override manuale (dovrebbe essere possibile risolvere comportamenti anomali con un “kill-switch”)
- Autenticazione! Almeno i comandi di guida dovrebbero essere autenticati
- Isolare i sistemi critici per la sicurezza dall'esterno (compresi gli update)



Per la privacy?

- Inserire informative semplificate e la possibilità di eliminare il maggior numero possibile di informazioni.
- Regolamenti settoriali per la protezione dei dati.
- In realtà è quasi impossibile resistere quando le pressioni vengono dalle autorità (statali o europee)



Grazie!

Ci sono domande?

Contatti:

a.guarino@studioag.eu



@alexsib17

Slide online su:
www.studioag.pro

StudioAG – Consulting & Engineering
www.studioag.eu

