PROCEDIMENTO DI PROTEZIONE DA ATTACCHI INFORMATICI AL VEICOLO E CORRISPONDENTE DISPOSITIVO

INVENTORI:
Rosadini Christian
Nesci Walter
Baldanzi Luca
Crocetti Luca
Fanucci Luca

CONTITOLARI: MAGNETI MARELLI S.P.A.

STATUS PATENT: CONCESSO

N° PRIORITÀ: 102018000021550

DATA DI DEPOSITO: 31/12/2018

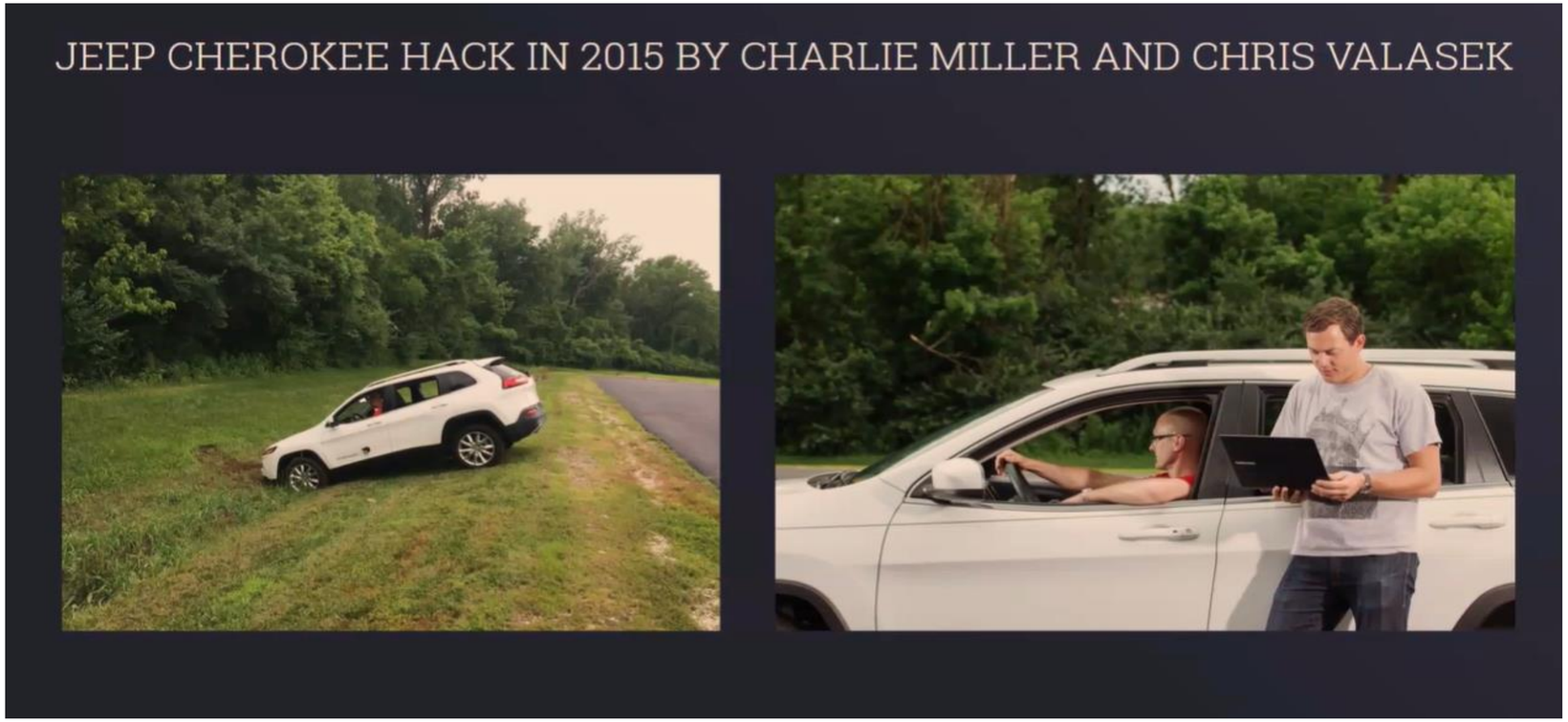
ESTENSIONE: IN201914048739, JP2020109953, CN111385286

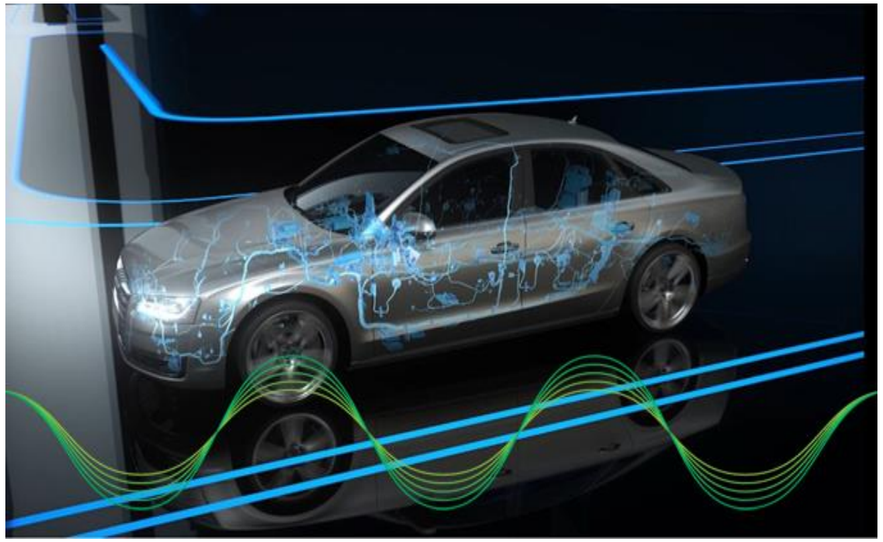
L'invenzione

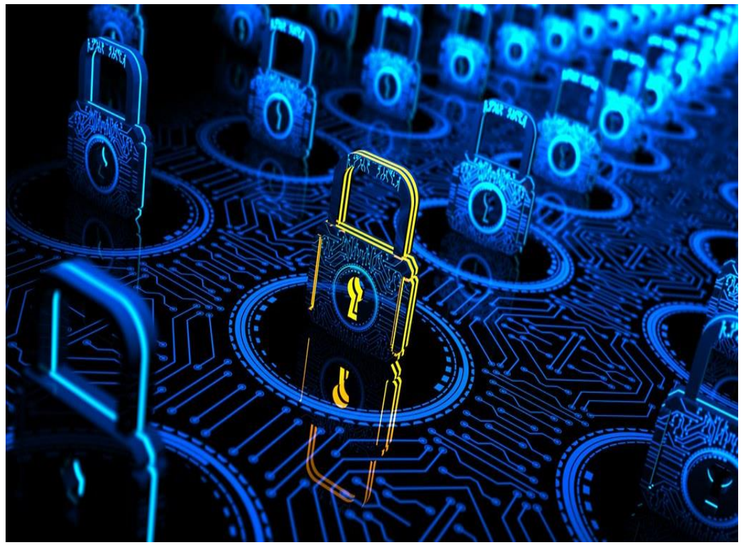
L'invenzione concerne tecniche di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) in un veicolo che adopera il sistema CAN-bus, l'impianto elettronico intelligente che sta sostituendo le vecchie centraline. Il sistema CAN-bus permette di **diagnosticare** in modo autonomo e intelligente **guasti e anomalie** e di notificarlo tramite messaggio o spia sul cruscotto. Questo sistema elettronico evoluto punta ad aumentare la **sicurezza** del veicolo attraverso un PC di bordo o centralina che controlla costantemente tutti i parametri vitali dell'auto. Proteggere questo tipo di sistema da possibili attacchi informatici è lo scopo dell'invenzione in oggetto.

Nel 2015 Charlie Miller e Chris Valasek, rispettivamente security engineer di Twitter e ricercatore di IOActive sono riusciti ad hackerare un Jeep Cherokee riuscendo ad inviare dei comandi attraverso il CAN-bus e hanno fatto fare tutto ciò che volevano a *qualsiasi* componente del veicolo. Sono riusciti a prendere il controllo del volante, del motore, della trasmissione, dei freni, per non parlare dei tergicristalli, dell'aria condizionata e della chiusura delle portiere. E hanno fatto tutto ciò in remoto, servendosi della rete cellulare Sprint. L'esperienza dei due ricercatori ha dimostrato la vulnerabilità del sistema e l'importanza di sistemi come l'invenzione da noi proposta per prevenire tali attacchi.

Disegni e Immagini







Applicabilità Industriale

L'invenzione si colloca nell'ambito della cybersecurity applicabile ai veicoli di nuova generazione. Il dispositivo e la procedura oggetto del brevetto permettono una serie di vantaggi:

- evitare il disallineamento temporale tra il messaggio corrotto (inviato sul bus) e il messaggio "Error-Frame" generato dal nodo CAN che riceve il messaggio corrotto;

- mascherare, attraverso un opportuno processo di offuscamento, 'operazione di corruzione al nodo CAN che ha inviato il frame illegale. Questo evita la ritrasmissione automatica, con conseguente occupazione del bus CAN, da parte del nodo CAN malevolo;

- non introdurre alcun ritardo di propagazione dei messaggi CAN, garantendo il loro utilizzo in modo trasparente da parte dei nodi CAN coinvolti;

- operare con messaggi CAN diagnostici. Grazie ad una logica di controllo dedicata, è possibile riconoscere una sequenza di messaggi diagnostici multi-frame e invalidare, se il servizio diagnostico viene identificato come malevolo, l'intera catena di messaggi.

Possibili Evoluzioni

È stato realizzato un prototipo della tecnologia in corso di validazione che è stato testato su veicoli reali. Il team di ricerca è interessato a collaborare con partners industriali per incrementare la maturità tecnologica dell’invenzione.

Per maggiori informazioni:

Ufficio di Trasferimento Tecnologico dell'Università di Pisa

Sede: Lungarno Pacinotti 43/44, Pisa (PI) 56126

Sito web: www.unipi.it/index.php/trasferimento

E-mail: valorizzazionericerca@unipi.it

Per maggiori informazioni:

Ufficio Regionale di Trasferimento Tecnologico

Sede: Via Luigi Carlo Farini, 8 50121 Firenze (FI)

E-mail: urtt@regione.toscana.it

UNIVERSITÀ DI PISA

REGIONE TOSCANA

urtt Ufficio Regionale di Trasferimento Tecnologico