UNIMORE Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

Piattaforma di test per attacchi e difese in reti in-vehicle

HackCar è una piattaforma di test progettata per replicare attacchi e difese alle reti interne dei moderni autoveicoli senza richiedere l'accesso a un veicolo completo di prova. La piattaforma consente di valutare in modo sicuro le conseguenze di attacchi mirati ai sistemi automobilistici su un ambiente realistico, facilitando lo sviluppo e la validazione di contromisure di sicurezza contro attacchi sia esistenti sia emergenti.
La piattaforma HackCar è basata su un modello **F1/10th**, al quale sono collegati diversi microcontrollori di grado automotive mediante protocolli di comunicazione tipici del settore automobilistico. L'architettura è progettata per essere completamente modulare, consentendo la definizione di molteplici scenari di test. In questo modo, ricercatori e professionisti possono sviluppare soluzioni di sicurezza innovative rispettando i vincoli imposti dai microcontrollori automotive-grade.

Laboratorio	CRIS
Area di specializzazione	Digitale, Meccatronica e Materiali
Referenti	Mirco Marchetti
Keyword	cybersecurity, automotive, cyber-physical system

"HackCar: Sicurezza automotive da simulazioni a test nel mondo reale"

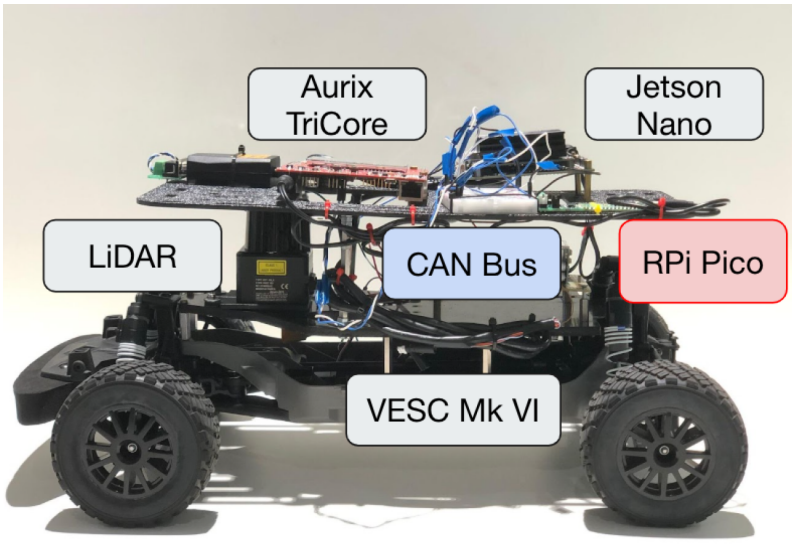


Fig. 1: Piattaforma di prototipazione HackCar

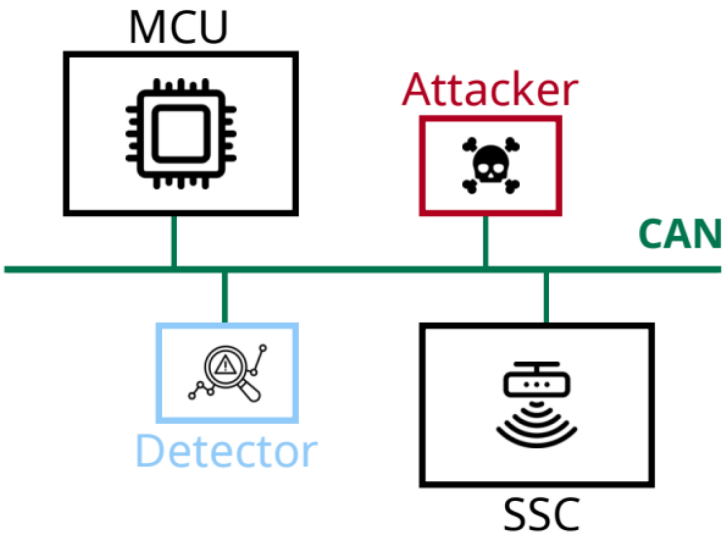


Fig. 2: Rappresentazione di alto livello dell'architettura di HackCar

Descrizione

HackCar è un prototipo rivolto a ricercatori nel campo della **cyber-security automotive**, sia in ambito accademico sia industriale. La piattaforma di prototipazione è dotata di sensori fisici, come **LIDAR**, e di **Electronic Control Unit (ECU)** che permettono l'implementazione di funzionalità ADAS comunemente diffuse, quali la frenata assistita e il cruise control adattativo.
A differenza di altre piattaforme miniaturizzate esistenti per lo sviluppo di applicazioni di guida assistita (ad esempio i modellini in scala F1/10th), HackCar replica l'architettura elettrica ed elettronica dei veicoli che comunemente circolano sulle nostre strade. Le ECU sono infatti interconnesse tramite un **CAN Bus**, elemento fondamentale per l'implementazione delle funzioni di guida assistita.
La presenza del CAN Bus consente di testare attacchi alle comunicazioni veicolari provenienti da attaccanti esterni o da ECU compromesse, nonché di valutare l'efficacia di meccanismi di sicurezza quali **secure gateway**, **intrusion detection system** e soluzioni basate sulla **crittografia**.

Aspetti innovativi

1- Replica realistica dell'architettura E/E automotive
HackCar si distingue dalle piattaforme F1/10th tradizionali replicando l'architettura elettrica ed elettronica dei veicoli di produzione, in particolare attraverso l'uso di ECU interconnesse tramite CAN Bus. Ciò consente di studiare problematiche di sicurezza in condizioni molto vicine a quelle reali.
Piattaforma fisica per la cyber-security veicolare
A differenza di approcci basati esclusivamente su simulazione, HackCar integra componenti fisici reali (sensori LIDAR, microcontrollori, bus di comunicazione), permettendo di analizzare l'impatto degli attacchi cyber direttamente sul comportamento del veicolo e sulle funzionalità ADAS.
Ambiente sicuro e controllato per test offensivi e difensivi
La piattaforma consente di condurre attacchi reali alle comunicazioni in-vehicle senza rischi per persone o veicoli, superando i limiti etici, legali ed economici dei test su automobili complete e omologate.
Modularità e flessibilità degli scenari di test
L'architettura modulare permette di configurare facilmente diversi scenari, rendendo HackCar adatta allo studio di minacce sia note sia emergenti.

Applicazioni

Ricerca in cyber-security automotive
HackCar può essere utilizzata per lo studio di attacchi al CAN Bus, alla comunicazione tra ECU e ai sistemi ADAS, nonché per la valutazione di contromisure quali intrusion detection system, secure gateway e meccanismi crittografici.
Sperimentazione industriale e prototipazione rapida
Aziende automotive e della sicurezza informatica possono utilizzare HackCar come banco di prova per prototipi di soluzioni di sicurezza.
Formazione e didattica avanzata
HackCar rappresenta uno strumento efficace per la formazione di studenti, ricercatori e professionisti.

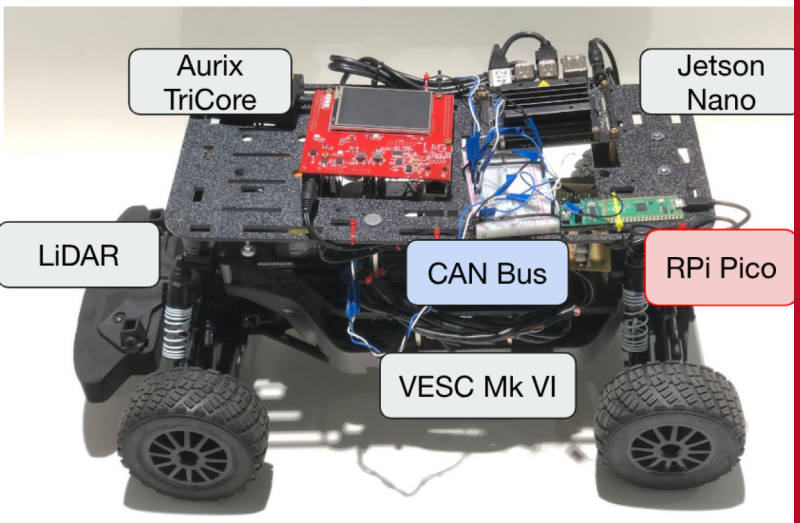


Fig. 3: Electronic Control Unit integrate sulla piattaforma HackCar

Partner coinvolti	Il prototipo è stato realizzato dal Centro di Ricerca Interdipartimentale sulla Sicurezza e la prevenzione dei rischi (CRIS) dell'Università di Modena e Reggio Emilia, in collaborazione con aziende del settore Automotive e Cybersecurity.
Tempi di realizzazione	da 1 a 6 mesi, a seconda della complessità
Livello di maturità tecnologica	TRL 7 - prototipo dimostrativo in ambiente operativo
Valorizzazione applicazione	Risultati preliminaru sulla piattaforma HackCar sono stati presentata alla converenza internazionale "IEEE Intelligent Vehicle Symposium", tenutasi nel 2024. L'articolo scientifico di riferimento è accessibile al seguente URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10588738

Esempio di applicazione

HackCar può essere utilizzata per testare attacchi al CAN Bus che compromettono una ECU ADAS, valutandone l'impatto su funzioni di frenata assistita e cruise control adattativo. La piattaforma consente di analizzare il comportamento del veicolo in uno scenario realistico e di validare contromisure come intrusion detection system e secure gateway in modo sicuro e ripetibile.

Risultati attesi dall'applicazione HackCar

1. Impatto sugli ADAS

• Osservazione degli effetti di attacchi sul CAN Bus e sulle ECU.
• Valutazione di malfunzionamenti o comportamenti anomali in funzioni critiche come frenata assistita e cruise control adattativo.
• Quantificazione del degrado delle prestazioni delle funzioni di guida assistita sotto attacco.

2. Validazione delle contromisure di sicurezza

• Test dell'efficacia di **intrusion detection system**: rilevamento di attività anomale, tempo di risposta, falsi positivi.
• Verifica di **secure gateway** e crittografia nelle comunicazioni interne, valutando prevenzione di manipolazioni senza compromissione della latenza o affidabilità.

3. Identificazione delle vulnerabilità

• Individuazione di ECU e percorsi di comunicazione più esposti a compromissioni.
• Analisi dei punti deboli della rete veicolare in scenari realistici.

4. Supporto a sviluppo e certificazione

• Generazione di evidenze sperimentali per migliorare architetture E/E e ADAS.
• Supporto alla definizione di linee guida per sistemi più sicuri e conformi a standard come ISO/SAE 21434.
• Possibilità di ottimizzare contromisure compatibili con vincoli hardware e software automotive-grade.

UNIMORE Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

CRIS

Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi



Il CRIS è stato fondato nel 2007 per riunire le diverse competenze sulla sicurezza disponibili in Ateneo. Il personale lavora a ricerche su problematiche legate alla sicurezza intesa in senso olistico, che spaziano dall'informatica, alla giurisprudenza, alla sicurezza sul lavoro, all'ambiente e ai materiali.
Il CRIS ha maturato particolare esperienza negli ambiti applicativi legati alla cyber security, al settore manifatturiero con specificità in ambito automotive, alla gestione di dati sensibili e alla privacy.
Promuove una visione globale della cultura della sicurezza fondata su tre aspetti: il fattore umano in senso stretto, quello scientifico-tecnologico e quello organizzativo-gestionale. È costituito dalle seguenti Unità Operative: Sicurezza informatica; Sicurezza fisica e Prevenzione dei rischi negli ambienti di lavoro industriali; Aspetti giuridici della sicurezza. La sua struttura interdipartimentale consente la valorizzazione, l'interazione e la contaminazione reciproca, promuovendo attività di disseminazione, formazione, ricerca e trasferimento tecnologico.
Le attività sono sostenute esclusivamente da contributi derivanti da ricerca e formazione e da fondi privati. I membri partecipano attivamente a numerosi progetti di ricerca e sviluppo con realtà aziendali del territorio, altre Università e Centri di livello regionale, nazionale e internazionale. I docenti sono regolarmente presenti nei Comitati Scientifici delle più prestigiose conferenze di diversi settori.

Sito web	http://cris.unimore.it
Direttore	Mirco Marchetti
Data pubblicazione	15/12/2025