ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

Scuola di Scienze

CORSO DI LAUREA IN INFORMATICA

TITOLO DELL'ELABORATO

CYBERSECURITY AUTOMOTIVE: ESSERE PROTETTI IN MOVIMENTO

RELATORE
Prof. Ozalp Babaoglu

PRESENTATA DA
Matteo Baldazzi

Sessione IV

ANNO ACCADEMICO 2021-2022

INDICE

INTRODUZIONE

Il presente elaborato tratta di un tema molto discusso in questi anni ovvero la Cybersecurity Automotive.

Per *Cybersecurity* si intende l'insieme di tecnologie e procedure atte alla protezione dei sistemi informativi. Il termine *Automotive* indirizza le strategie e le problematiche di sicurezza nell'ambito dell'industria automobilistica.

Con l'avanzata delle nuove tecnologie smart, anche il settore dei veicoli ha subito costante sviluppo. Le numerose innovazioni, infatti, hanno portato alla crescita esponenziale di autovetture interconnesse.

Purtroppo, però, l'aumento di connessioni determina un maggiore scambio di dati esposti al rischio di attacchi informatici che violano i principi di confidenzialità, integrità e disponibilità. Ciò implica la necessità di ricercare e sviluppare sistemi di sicurezza sempre più all'avanguardia in modo da garantire privacy e tutelare l'utente.

Inoltre, l'evoluzione è indirizzata verso la creazione di veicoli intelligenti, in particolare macchine dotate di guida assistita o anche autonoma. Questo comporta grandi vantaggi e comodità ma, sfortunatamente, anche la possibilità che qualcuno al di fuori del conducente prenda il controllo dell'autovettura ed esegua comandi (ad esempio frenare, aprire le portiere, …), provocando gravi conseguenze e danni fisici.

Molte persone ritengono che la cybersecurity sia un argomento proiettato su un futuro ancora astratto; in realtà, al giorno d'oggi sono già molti i casi di attacchi informatici. Pertanto, è molto importante per le diverse entità sapere come e quanto tutelarsi e difendersi.

La tesi, in particolare, spiega varie fonti di possibili minacce prima in generale e poi del mondo automotive, elencando possibili attacchi da parte di terzi. Richiama anche l'attenzione su quanto la cybersecurity sia importante fin dalla progettazione di un prodotto e non solo un elemento che può essere preso in considerazione alla fine; l'identificazione e prevenzione di queste minacce tramite tecniche e standard come il NIST Framework, garantisce una maggior affidabilità e sicurezza.

Effettua anche un’analisi del IoV ovvero la comunicazione autonoma dei veicoli con altri elementi esterni (infrastrutture, veicoli, …) con lo scopo di migliorare le funzionalità digitali del veicolo e specialmente migliorando la guida autonoma.
Come ultimo punto fornisce l’approfondimento del Digital Twin, una tecnologia già utilizzata in altri settori ma inserite negli ultimi anni nella produzione automobilistica e ancora più di recente nella vita di un veicolo mentre è su strada. Questa tecnica aiuta a prevenire e contrastare malfunzionamenti o cyber-attack, nel mondo più veloce ed efficace possibile.

1. Cybersecurity

La cybersecurity è la pratica che consente a un'entità (ad esempio organizzazioni, cittadini, nazioni, imprese, ecc.) di proteggere i propri asset dalle minacce che arrivano dal cyberspace e di preservare la confidenzialità, l'integrità e la disponibilità delle proprie informazioni.
Nello specifico, si tratta del processo che consente la protezione attraverso azioni di prevenzione, rilevazione e risposta ad attacchi informatici
Pertanto, per *cybersecurity* non si intende solo l'aspetto tecnologico, bensì l'insieme delle attività, dei ruoli, delle responsabilità e delle metodologie idonee a garantire la gestione del Cyber Risk.

1.1 Cyber Risk

Per *cyber risk* si intende il rischio derivante dal cyberspace e dai sistemi informatici. Come tutti i rischi di diversa natura, anche il cyber risk è collegato alla possibilità di perdere qualcosa di valore. Il rischio, infatti, nella sua definizione generale, è legato all'incertezza del verificarsi di eventi prevedibili o improvvisi, diretti o indiretti, misurabili o non misurabili. Tale incertezza è legata sia agli eventi stessi che alle loro cause ed effetti, non sempre facilmente identificabili e definibili.
Indipendentemente dalla tipologia di rischi, c'è una certa convergenza sul definire il rischio come la materializzazione di un evento negativo che possa compromettere il raggiungimento di obiettivi aziendali. Esso può essere visto come il risultato di tre fattori: la minaccia, la vulnerabilità e l'impatto.

- Minaccia: per "minaccia" si intende una fonte di rischio, ovvero un evento che potrebbe recare un danno di qualsiasi natura all'azienda.
- Vulnerabilità: la "vulnerabilità" corrisponde a quanto si è deboli rispetto ad una determinata minaccia. Quando la vulnerabilità è bassa vuol dire che si è molto

protetti, ogni azienda può essere più o meno vulnerabile rispetto ad una determinata minaccia.

- Impatto: nel caso in cui le nostre difese non siano sufficienti per proteggersi da una minaccia, con "impatto" si intende l'analisi di quali conseguenze potrebbero insorgere e l'entità del danno che potrebbero portare all'impresa.

1.1.1 Fonti di rischio

Il cyber risk è suddiviso in due tipologie:

1. *First party risk*
2. *Third party risk*

Il *first party risk (*"rischio dei propri asset") è quello che genera un impatto diretto sull'azienda non coinvolgendo altri soggetti, mentre il *third party risk* ("rischio verso terzi") si riferisce alle passività subite da parti terze e imputabili alla vittima.
Delle due tipologie di rischio, il *third party risk* risulta essere il più grave e anche quello che più preoccupa le aziende, poiché non dipende da eventi certi che si possono verificare internamente, bensì dipende da fattori esterni specialmente provenienti dal web.
A questo proposito, i rischi legati al mondo web sono otto:

1. *Errore dovuto alla normale attività di comunicazione tramite i social network aziendali*: le aziende utilizzano sempre più i social network (Facebook, Twitter, ...) principalmente per effettuare campagne pubblicitarie e per accrescere la loro notorietà. L'errore dell'impiegato responsabile dell'account dei social network, come ad esempio la pubblicazione di un post non conforme agli interessi dell'azienda, potrebbe comprometterne la reputazione e causare una riduzione delle vendite dovute ad una minor fidelizzazione del consumatore.
2. *Gossip o pettegolezzi nei social media*: il successo di un'azienda verte anche sul positivo riscontro che ha nei confronti dei consumatori; quindi, la pubblicazione

su forum di voci maliziose sui prodotti o sui servizi della società mettono a rischio la reputazione della stessa. Le voci si diffondono a livello virale in modo talmente tempestivo da raggiungere la sfera internazionale e i media tradizionali.

3. *Sequestro di account di social media*: si tratta di veri e propri *cyber crime* posti in essere da hacker per sequestrare gli account dei social media dell'azienda e utilizzarli in maniera inopportuna, danneggiando l'immagine e la reputazione aziendali. In aggiunta, il tutto può essere seguito da minacce e richieste di riscatto.
4. *Il sito web della società è "craccato"*: un gruppo di hacker attacca il sito di una società avvalendosi di attacchi di tipo DDoS riuscendo ad oscurare il sito per più di un giorno con una serie di conseguenze gravi.
5. *Cyber-spionaggio*: si tratta di azioni condotte da hacker esterni o da insider per sottrarre informazioni fondanti per le aziende. Ad esempio, un'azienda concorrente potrebbe utilizzare i canali della rete per accedere a informazioni riservate riguardanti nuove strategie aziendali d'investimento sui prodotti. Ne consegue che il vantaggio competitivo della società colpita è messo a rischio. L'attacco potrebbe persino consentire alla società concorrente di rimarginare il divario esistente e magari anche di sorpassare l'azienda colpita da cyber-spionaggioa livello competitivo.
6. *Perdita di dati*: a causa di uno sbaglio o di un errore procedurale, una società perde le informazioni riguardanti dati sensibili, come ad esempio dati relativi alle carte di credito o dati personali di un numero significativo di clienti. Di conseguenza, la stampa apprende la notizia, perché la società è costretta a notificare la perdita dei dati. L'incidente danneggia gravemente la reputazione aziendale, compromettendo anche la fidelizzazione dei clienti.
7. *Furti digitali*: anche in questo caso si tratta di un esempio di *cyber crime*. Infatti, può accadere che un'organizzazione criminale riesca a oltrepassare le protezioni online di una società e a rubare informazioni rilevanti su carte di credito o dati personali dei clienti contenuti nel database, mettendoli in vendita online. Tutto

questo costituisce un danno per la società in quanto i clienti perdono rapidamente la fiducia nel sistema di sicurezza dell'azienda e il rapporto commerciale con la stessa.

8. *Casus belli per una guerra*: due o più Paese entrano in guerra a seguito di un casus scatenato tramite la rete. Un Paese tenta di scardinare le reti informatiche del Paese vicino, al che quest'ultimo risponde con misure di guerra convenzionali. Oltre a compromettere i collegamenti Internet in tutta la regione e a interrompere totalmente il commercio online, il conflitto può degenerare in una guerra convenzionale.

1.1.2 Danni del cyber risk

I fattori di rischio cyber possono provocare diverse tipologie di danni ai quali le aziende devono far fronte.

A tal riguardo possiamo distinguere tre grandi famiglie di danni:

1. *Danni materiali diretti ed indiretti*: riguardano i danni (distruzione parziale o totale, furto) subiti da beni materiali, quali ad esempio un server, la fibra ottica, i computer, un cellulare, ... Prendendo in esame le polizze assicurative contro questa tipologia di danni, dal momento che i danni si manifestano su beni tangibili, si può dire di non essere necessariamente oggetto di una copertura specifica sul *cyber risk*. Infatti, proprio per la loro natura diretta e fisica, questa tipologia di danni potrebbero già rientrare in una polizza assicurativa più generale, per la copertura degli asset materiali.
2. *Danni immateriali diretti ed indiretti*: parlando di danni immateriali, questi rappresentano i tipici danni causati dal *cyber risk*. Infatti, i sinistri informatici sono caratterizzati dall'immaterialità. I danni di natura informatica colpiscono beni non tangibili, ma comunque funzionali ed indispensabili allo svolgimento di una qualsiasi attività aziendale. All'interno di questa tipologia di danni abbiamo distinto i danni diretti da quelli indiretti. Il danno immateriale diretto

può essere tradotto nell'impossibilità dell'azienda a continuare la sua attività; tuttavia, al contrario di quanto avviene in un sinistro "tradizionale", spesso l'interruzione dell'attività aziendale è pervasiva, tende a diffondersi in modo omogeneo e può colpire anche sedi remote. Il danno immateriale indiretto, invece, si riferisce al danno relativo alla perdita d'immagine e reputazione aziendale, nonché alla perdita di quote di mercato.

3. *Danni Property (risarcimento per responsabilità)*: quest'ultima tipologia di danno riguarda soprattutto quelle aziende che offrono servizi informatici (ad esempio gestione dell'infrastruttura IT di un'azienda cliente) che hanno subito una problematica cyber, causando l'interruzione della fornitura dei servizi informatici nei confronti di terzi. Tali società devono, quindi, considerare il danno relativo alle richieste di risarcimento da parte dei clienti, che a livello aziendale si traduce in un extracosto da sostenere per soddisfare la richiesta di un terzo.

1.1.3 Risk Management

Il risk management ("gestione dei rischi") ha lo scopo di proteggere l'azienda dai rischi che possono presentarsi e dalle loro conseguenze dannose che creano una reazione a catena che si propaga all'interno e all'esterno dell'organizzazione.
Questo processo si divide in tre fasi: identificazione, valutazione e gestione.
La prima fase è quella dell'*identificazione* dei rischi, nella quale vengono raccolte ed elaborate tutte le informazioni necessarie a descrivere il profilo di rischio aziendale. Occorre, senza fare stime eccessive o insufficienti, mettere in evidenza:

- le unità di rischio, cioè le risorse aziendali che potenzialmente possono essere oggetto di eventi dannosi;
- i pericoli, cioè le cause di eventi sfavorevoli che possono colpire le risorse;
- le causalità, cioè le condizioni che favoriscono il verificarsi dell'evento negativo;

- le tipologie di effetti che ogni evento dannoso può provocare.

Per essere eseguita è necessaria da parte del risk manager un'approfondita conoscenza della realtà aziendale in modo da poter individuare le interrelazioni tra le parti, i punti di forza e di debolezza, le reazioni a catena che potrebbero verificarsi.
Come seconda fase abbiamo la *valutazione dei rischi*, che consiste nell'identificazione della frequenza, della gravità e delle perdite potenziali relative ai rischi esaminati e nell'attuazione di analisi di convenienza tra diverse alternative di gestione volte a minimizzare il costo. Si tratta di determinare una funzione matematica f del tipo: R = f (M, P), dove R è la magnitudo del rischio, M è la magnitudo delle conseguenze e P è la probabilità o frequenza del verificarsi delle conseguenze. In questa fase vengono confrontate le diverse tecniche di gestione, considerando scenari alternativi, in modo da giungere a una soluzione ottimale in termini di efficienza e di efficacia.
Per ultima fase troviamo la *gestione* dei rischi che consiste nella selezione, in base ai costi e ai risultati attesi, degli strumenti da applicare per rendere il rischio economicamente accettabile e nella realizzazione concreta di quelli selezionati. Le tecniche di gestione possono essere distinte in tecniche di controllo, che agiscono direttamente sulle determinanti del rischio e in tecniche di finanziamento, che nell'ipotesi del verificarsi dell'evento dannoso agiscono sulle conseguenze economico-finanziarie di quest'ultimo. Le tecniche di controllo comprendono la prevenzione e la protezione attraverso l'uso di misure di sicurezza fisiche, di procedure e di formazione. Le tecniche di finanziamento trattano dell'individuazione dei mezzi finanziari necessari a fronteggiare le spese o gli investimenti per il ripristino della capacità produttiva perduta in seguito al sinistro.
In conclusione, attraverso l'identificazione, la valutazione e la gestione dei rischi, il risk manager ha il compito di rendere il profilo di rischiosità dell'impresa coerente con i suoi obiettivi, anche mediante la collaborazione, la comunicazione e l'integrazione con altre funzioni aziendali.

1.2 Sicurezza dei dati

Ormai qualsiasi informazione, di qualsiasi tipologia, riguardante qualsiasi ambito è digitalizzata ovvero immagazzinata sotto forma di dati; questo comporta che la protezione e la conservazione siano due fattori essenziali per qualsiasi entità.
La sicurezza si sviluppa attorno all'acronimo CID (CIA in inglese) composto da tre elementi fondamentali:

- *Confidenzialità*: è la proprietà in virtù della quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi che non sono autorizzati;
- *Integrità*: la proprietà di salvaguardia dell'accuratezza e della completezza degli asset.
- *Disponibilità (Availability):* proprietà in virtù della quale le informazioni sono rese accessibili e utilizzabili su richiesta di una entità autorizzata;

Ogni evento, casuale o no, viola la sicurezza di un dato quando infrange almeno uno di questi tre cardini della cybersecurity. Esistono vari tipi di minacce possibili ed incentrate proprio sull'attaccare questi tre dogmi della protezione informatica; tra i più comuni abbiamo:

- *Malware*: il termine deriva dall'abbreviazione di *malicious software* (software dannoso), indica un qualsiasi software usato per disturbare le operazioni svolte da un computer: rubare informazioni sensibili, accedere a sistemi informatici privati, mostrare pubblicità indesiderata, distruggere e ottenere dati. All'interno di questa macrocategoria troviamo: virus, worm, trojan, ransomware, spyware, adware, shareware, e altri programmi malevoli. Il malware si diffonde principalmente inserendosi all'interno di file non malevoli. Il malware non necessariamente è creato per arrecare danni tangibili ad un computer o un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo.

- *Sniffing*: consiste nel “annusare” i pacchetti durante il loro trasferimento in rete così da ottenere informazioni che dovrebbero restare confidenziali.
- *Phishing*: è un tipo di truffa effettuata su Internet, attraverso la quale il malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. La tecnica utilizzata è molto semplice: viene effettuato un invio massivo di messaggi di posta elettronica o in alcuni casi di SMS, simili nell’aspetto e nel contenuto ai messaggi dei fornitori di servizi. Questi messaggi fraudolenti richiedono informazioni riservate: il numero della carta di credito, le password per accedere a un determinato servizio, ...
- *Password attack (attacco a dizionario)*: si tratta del tentativo di ottenere la password di un utente per avere alcuni privilegi di accesso. Nella crittoanalisi e nella sicurezza informatica, un attacco a dizionario è una tecnica di attacco alla sicurezza di un sistema, o sottosistema informatico, mirato a “rompere” un codice cifrato o un meccanismo di autenticazione. Il tentativo è quello di provare a decifrare il codice o di determinare la password, cercando tra un gran numero di possibilità. In pratica, si cerca di accedere a dati protetti da password (sia remoti, come ad esempio account su siti web o server di posta, database server, sia locali, come documenti o archivi protetti da password) tramite una serie continuativa e sistematica di tentativi di inserimento della password, solitamente effettuati in modo automatizzato, basandosi su uno o più dizionari.
- *Denial of service*: tradotto in italiano con “negazione del servizio” e talvolta abbreviato in DoS, è una minaccia informatica il cui obiettivo primario è quello di interrompere i servizi di rete o web di un’azienda, facendo esaurire le risorse informatiche di un sistema che fornisce un servizio ai client, fino a renderlo inutilizzabile. Sono attacchi principalmente volti a danneggiare una società o la reputazione di un marchio.

- *Man in the middle*: indica un tipo di attacco crittografico nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti comunicanti tra di loro.
- *Drive-by download*: è un termine utilizzato con due diverse accezioni: nella prima si tratta di un download automatico con conseguente installazione di un file malevolo nel momento stesso in cui l'utente accede a un sito, senza alcune interazioni dell'utente stesso; nella seconda il download viene autorizzato dall'utente facendogli credere di scaricare un programma sicuro o una applicazione, che si rivela essere un malware. Questa tipologia di attacco si può concretizzare nel momento in cui si visita un sito web, un messaggio di posta elettronica o cliccando su una finestra pop-up ingannevole.
- *Rogue*: anche noto come fraudtool (letteralmente "strumento di frode"), è una particolare categoria di malware che finge di essere un programma noto, o comunque non malevolo (ad esempio un Antivirus), al fine di rubare dati confidenziali o di ricevere denaro. Questi malware hanno anche, al loro interno, funzionalità di adware. [Citazione]

1.3 Black Market

Ma quindi perché sempre con più frequenza le aziende subiscono attacchi?
Esiste un mercato nascosto chiamato *Mercato Nero* nel quale le risorse principali e più vendute sono indubbiamente i dati; infatti, le società che possiedono le informazioni degli utenti presentano valutazioni maggiorate. Dato che il valore commerciale dei dati è in crescita, negli ultimi tempi i criminali informatici sono artefici del cybercrime-as-a-service, fondando una vera e propria economia basata sulla vendita dei dati rubati. Si tratta di un sistema che offre la possibilità di accedere al cybercrime acquistando vari servizi, dai pacchetti di attacco cyber preconfezionati fino ad interi database di e-mail e altri dettagli personali. Attorno a questa nuova tendenza si sviluppano le dinamiche

tipiche del business moderno, veri e propri marketplace dove si sfruttano strategie di marketing e CRM.
Le principali tipologie di dati sono tre: dati personali, medici e finanziari.

1.3.1 Dati personali

La pubblicazione speciale 800-122 del NIST riprende la definizione di Personally Identifiable Information, ovvero tutte le informazioni su un individuo mantenute da un'agenzia, tra cui tutte quelle che possono essere utilizzate per distinguerne o tracciarne l'identità, come: nome, numero di previdenza sociale, data e luogo di nascita, nome da nubile della madre, dati biometrici e qualsiasi altra informazione alla quale è collegato o collegabile ad un individuo, come dati medici, educativi (scolastici), finanziari e informazioni sull'occupazione.

1.3.2 Dati Medici

Strettamente legato al mercato delle identità rubate è quello delle informazioni mediche ottenute illecitamente. Un esempio di sottrazione illecita di informazioni di questo tipo è riportato in Figura 1.1. In questo caso il truffatore ha messo in vendita, sul noto online

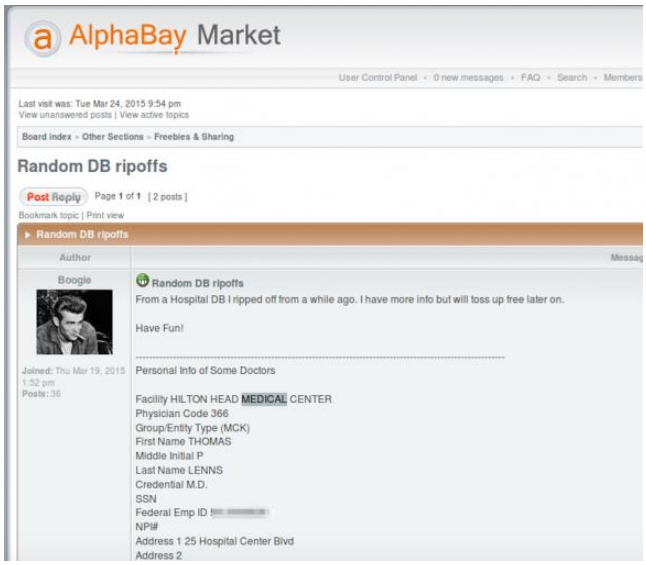

Fig. 1.1 Un esempio di informazioni rubate da un servizio sanitario e messe in vendita [15].

darknet market Alpha Bay, un file di testo di grandi dimensioni contenente nomi, indirizzi, codici fiscali e altri dati sensibili su decine di medici dell'ospedale Hilton Head Medical Center. Altri tipi di attacchi rivolti a strutture medico-sanitarie consistono in una richiesta di riscatto a seguito di una criptazione dei dati sensibili, grazie all'uso di specifici ransomware.

1.3.3 Dati Finanziari

Il furto di dato finanziario più diffuso è quello degli estremi delle carte di pagamento, la cui sottrazione indebita colpisce particolarmente i commercianti. Il prezzo delle carte di pagamento, messe a disposizione in questi mercati, varia in base alle informazioni disponibili insieme al numero della carta di pagamento:

- Il codice di verifica della carta CVV. CVV1 è il codice univoco a tre cifre contenuto nella banda magnetica della carta. CVV2 è il codice a tre cifre stampato sul retro della carta.
- Combinazione valida di numero di account primario (PAN), data di scadenza e codice CVV2 generata dal software. I generatori di numeri di carte di credito possono essere acquistati o reperiti gratuitamente online.
- Numero di carta scelto casualmente all'interno di un database violato, ed è casuale in merito a banca e tipo di carta.
- Tutti i dettagli della carta e del suo proprietario, come nome completo, indirizzo di fatturazione, numero della carta di pagamento, data di scadenza, codice PIN, codice fiscale, cognome da nubile della madre, data di nascita e CVV2. Possono includere anche il nome utente e password associati ad home banking. Con queste ultime credenziali il compratore può modificare l'indirizzo di spedizione o di fatturazione oppure aggiungerne altri.

2. Ambiente Automotive

Ogni anno ci sono enormi sviluppi di nuove applicazioni e servizi automobilistici che stanno guidando la produzione in termini di costi e tecnologia. Oltre il 90% delle invenzioni automobilistiche porta a innovazioni nell'hardware e nel software del veicolo. L'hardware nei veicoli ha un sistema di controllo, che li indirizza a svolgere vari compiti sulle strade durante la guida.
Queste attività si dividono in tre categorie a seconda di che cosa gestiscono:

- Sistemi primari, ad esempio motore, assistenza alla guida, trasmissione, impianto elettrico, impianto frenante, cruscotto, ecc.
- Sistemi secondari, ad esempio accensione, indicatori, controllo dei finestrini, tergicristalli, luci…
- Applicazioni di infotainment, ad esempio sistemi di navigazione, telematica, intrattenimento per i sedili posteriori, intrattenimento musicale e video e servizi basati su GPS.

I moderni progressi nel settore elettrico ed elettronico hanno cambiato radicalmente l'industria automobilistica. Questi veicoli non sono più sistemi completamente meccanici dopo l'intervento dell'elettronica. Inoltre, questi dispositivi elettronici hanno aggiunto una serie di funzionalità inimmaginabili, migliorando le prestazioni complessive dei veicoli.
Al giorno d'oggi, i veicoli sono più veloci, più sofisticati, con nuove funzionalità e più efficienti. Questi progressi sono il risultato di dozzine di centraline elettroniche (ECU) e di una vasta rete di comunicazione che le interconnette e consentono un'esperienza di guida completamente nuova: dai veicoli che possono essere bloccati e sbloccati a distanza, ai veicoli che possono essere guidati senza una chiave nell'accensione e possono persino guidare o parcheggiare da soli. Questa nuova esperienza di guida si ottiene utilizzando centinaia di megabyte di codice contenuti nelle centraline del veicolo. Si possono trovare i veicoli senza conducente di Google che si guidano da soli

in Nevada e sono consentiti anche in Florida e California. Quindi è solo una questione di tempo prima che vedremo veicoli più autonomi e intelligenti in tutto il mondo, probabilmente aumentando la sicurezza di guida; tuttavia, per quanto riguarda gli aspetti di sicurezza?

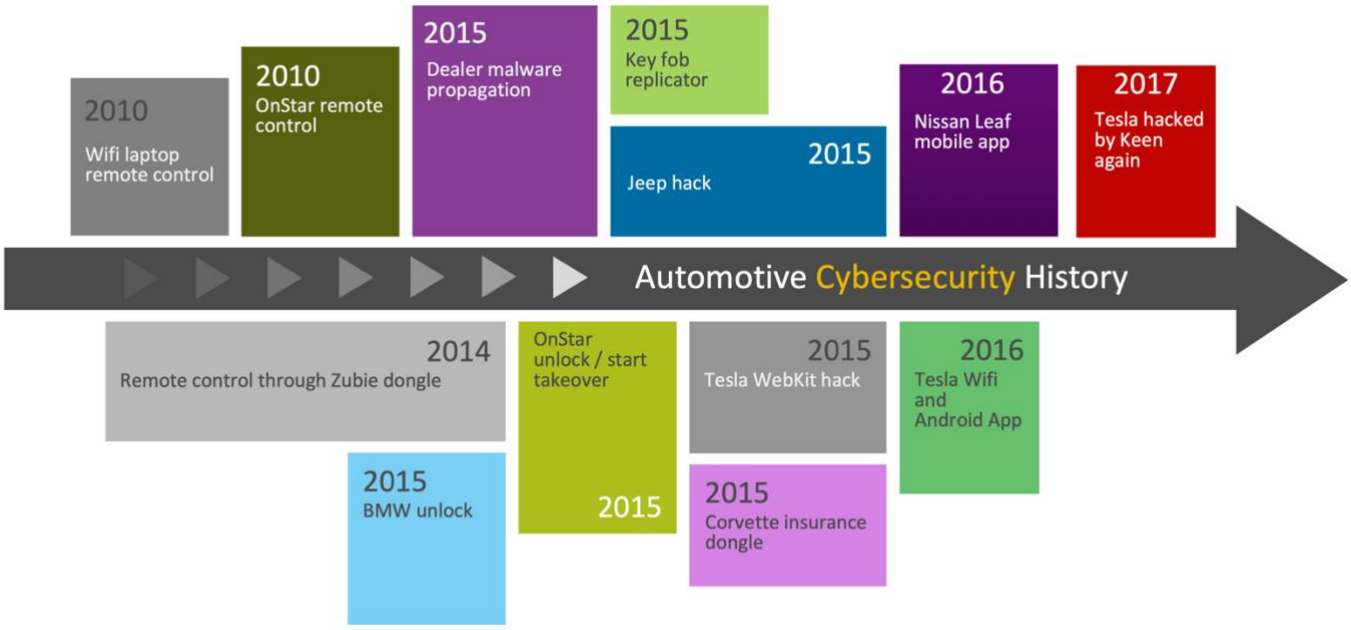

Fig. 2.1 Linea del tempo della Cybersecurity Automotive

2.1 Minaccia crescente

Con lo sviluppo delle tecnologie, vengono eseguite sempre più azione automatiche mediante componenti elettroniche e non più solo meccaniche, come la frenata di emergenza, accelerazione e decelerazione automatiche tramite il cruise control adattivo, e addirittura ad oggi abbiamo veicoli con guida autonoma.

Considerando che queste innovazioni hanno un gran potere sulla vettura diventa sempre più importante proteggerle da attacchi, infatti, diventa necessario applicare protocolli di sicurezza per tutelarle da qualsiasi tipo di minaccia che potrebbe compromettere la protezione della vettura o dei passeggeri.

Possiamo osservare nella Fig. 2.1 alcuni eventi che hanno segnato la storia della sicurezza informatica automobilistica.

Ogni autovettura utilizza componenti hardware per controllare le operazioni

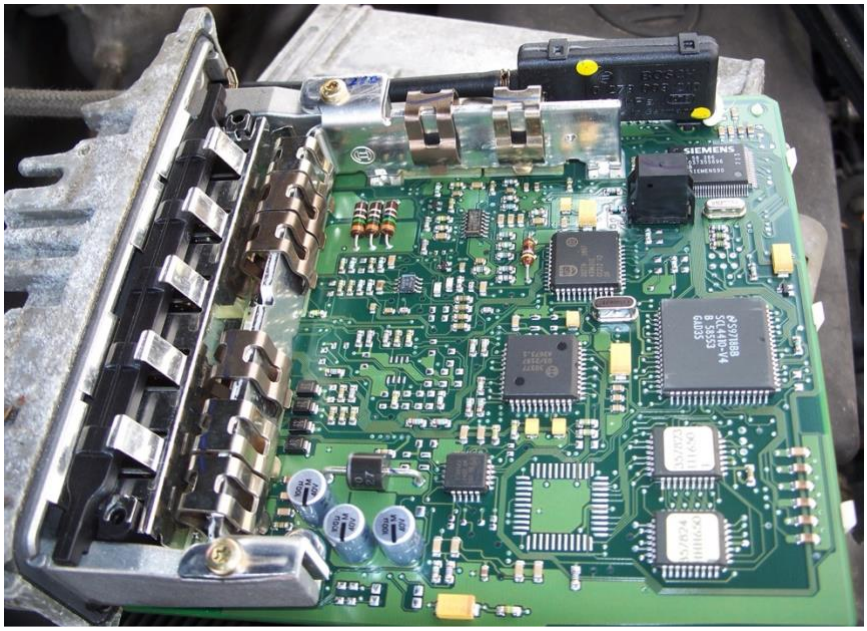

Fig. 2.2 ECU di una Volkswagen Golf

elettroniche tra le più conosciute abbiamo la ECU (Engine Control Unit) e l'ABS (Anti-lock Braking System).

Questi dispositivi svolgono compiti sempre più complessi aggiungendo vantaggi e sicurezza da un lato ma complicando la protezione del veicolo, perché introducono potenziali vettori di attacco al sistema.

Per comunicare le une con le altre, queste centraline sono dotate di varie tecnologie come Ethernet, reti cellulare, Wi-fi, Bluetooth ecc. tutte utilizzate nei veicoli moderni, di conseguenza per rendere un sistema protetto non è sufficiente mettere in sicurezza tutte le componenti singolarmente, bensì è necessario proteggere anche tutti i canali di comunicazione che utilizzano per "parlare" tra loro.

Attualmente, i problemi di sicurezza informatica stanno peggiorando ulteriormente. I veicoli possono essere hackerati o immobilizzati a distanza, possono essere compromessi attraverso sensori e la persona può essere ferita fisicamente se qualcuno si impossessa del veicolo e lo arresta improvvisamente.

2.2 Veicoli Intelligenti e Autonomi

La storia dei veicoli intelligenti, al contrario di quello che si pensa, è iniziata negli anni Ottanta quando la azienda DARPA (Defense Advanced Research Projects Agency) presentò il primo sistema di trasporto intelligente (ITS, Intelligent Transportation System) chiamato AVL (Autonomous Land Vehicle); questo, sfruttando la "computer vision", "Light Detection And Ranging" (LiDAR) e "Global Positioning System" (GPS), riusciva a muoversi autonomamente con la completa assenza di un guidatore [4].

Col tempo è stata aggiunta della vera e propria intelligenza artificiale all'interno dei veicoli, rendendoli in grado effettuare calcoli e prendere decisioni di conseguenza in modo autonomo, così nacquero i veri e propri Veicoli Intelligenti (VI), fino ad oggi dove abbiamo sistemi pensanti in movimento collegati con ciò che li circonda.

In particolare, le connessioni si dividono in due grandi categorie:

- "Short Range": sfruttano le connessioni a corto raggio e le onde per mettere in comunicazione "veicoli-veicoli" (V2V) e "veicoli-infrastrutture" (V2I) poi estese a veicoli a tutto (V2X).
- "Long Range": utilizzano le tecnologie cellulare (es. LTE e 5G) per collegare il mezzo ad Internet implementando anche l'IOT (Internet of Things).

Con queste tecnologie Google è riuscita a creare veicoli autonomi per tracciare le loro mappe e Tesla è riuscita a creare un'automobile con la possibilità di guida autonoma.

2.2.1 Classificazione dei veicoli con guida autonoma

Quando parliamo di guida autonoma non significa per forza che sia "completamente" autonoma, infatti, esistono delle classificazioni che attribuiscono il livello di indipendenza del veicolo, ovvero le azioni che può eseguire senza la necessità che il conducente intervenga. Esistono due società principali che hanno stabilito i livelli di

autonomia: SAE (Society of Automotive Engineers) e NHTSA (National Highway Traffic Safety Administration).

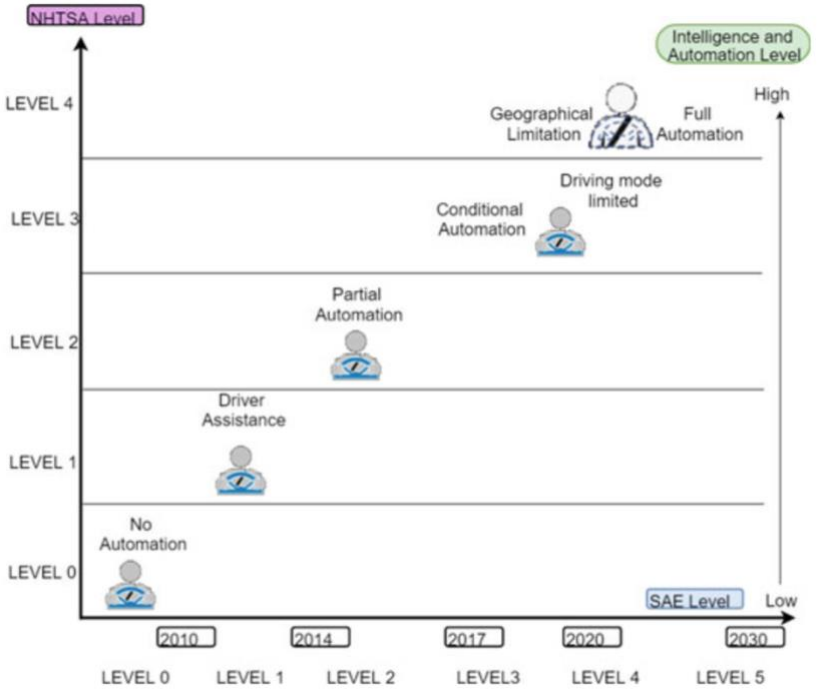

Fig. 2.2 Confronto tra i livelli di SAE e NHTSA

Come è mostrato dalla Fig. 2.2 le due scale di livelli sono equivalenti per il livello 0, livello 1 e livello 2 per poi variare leggermente nei livelli successivi.

Considerando che la maggior parte di case automobilistiche come Tesla, Nissan, Toyota seguono lo standard di SAE International è doveroso approfondire i livelli.

La assegnazione ad un determinato livello si ha in base alla necessità di intervento da parte del guidatore se si presenta una certa condizione. Nei livelli 0,1 e 2 il conducente deve guidare a tutti gli effetti anche se alcune funzionalità lo aiutano; infatti, questi livelli sono definiti come "guida assistita" e possono intervenire su azioni basilari. Dal livello successivo si passa a "guida autonoma" con delle sfumature però; a livello 3 il veicolo può richiedere al conducente di intervenire nel caso qualcosa vada storto ed anche se questo non stava guidando deve essere vigile e pronto; a livello 4 invece arriviamo a una guida completamente autonoma in alcune condizioni specifiche al

contrario del livello seguente che è interamente autonomo in qualsiasi condizione, ha solo la necessità di comunicare al veicolo la destinazione.

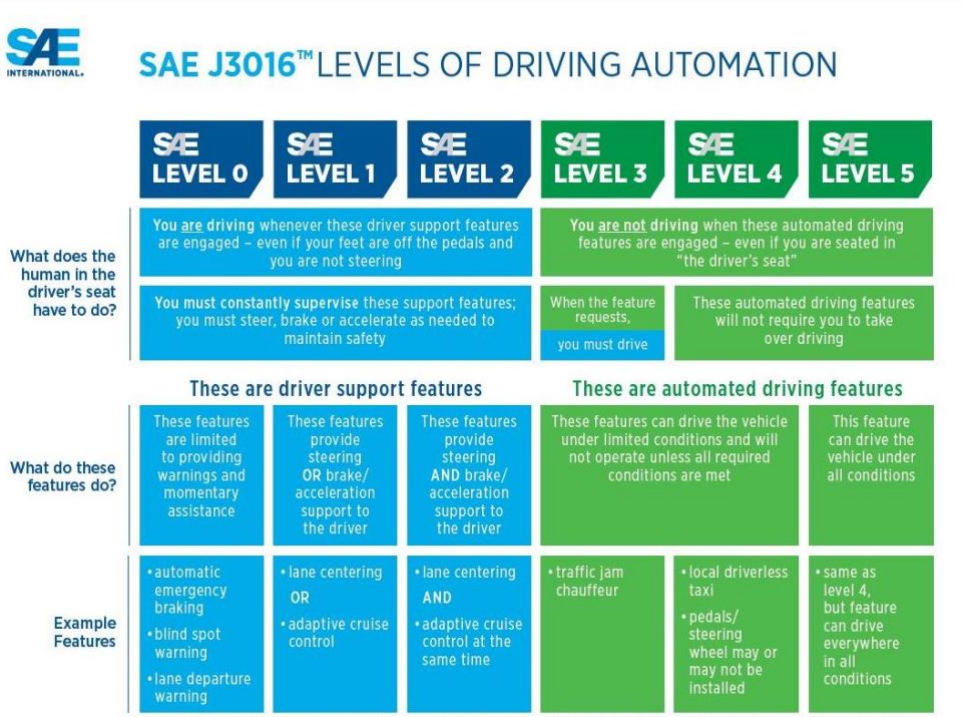

Fig. 2.3 Specifica livelli SAE [citazione sito]

2.2.2 Comunicazione interna ed esterna

Come detto in precedenza ogni veicolo per appartenere alla categoria IAV (Intelligent and Autonomous Vehicles) è fornito di moltissime tecnologie diverse che per essere efficienti hanno bisogno di comunicare tra loro, è questa interazione mescolata ad algoritmi di Intelligenza Artificiale (IA) e Machine Learning (ML) che riesce a rendere la vettura in grado di scegliere e compiere azioni.

Il sistema di comunicazione è diviso in due grandi architetture, una per la comunicazione interna al veicolo ed una per quella esterna.

La comunicazione all'interno si riferisce alla trasmissione di informazioni tra tutti i componenti interni come radar, sensori, attuatori e centraline. Questa sfrutta principalmente canali cablati dato che per raggiungere una guida autonoma efficiente sono necessarie alta velocità e affidabilità di trasmissione.

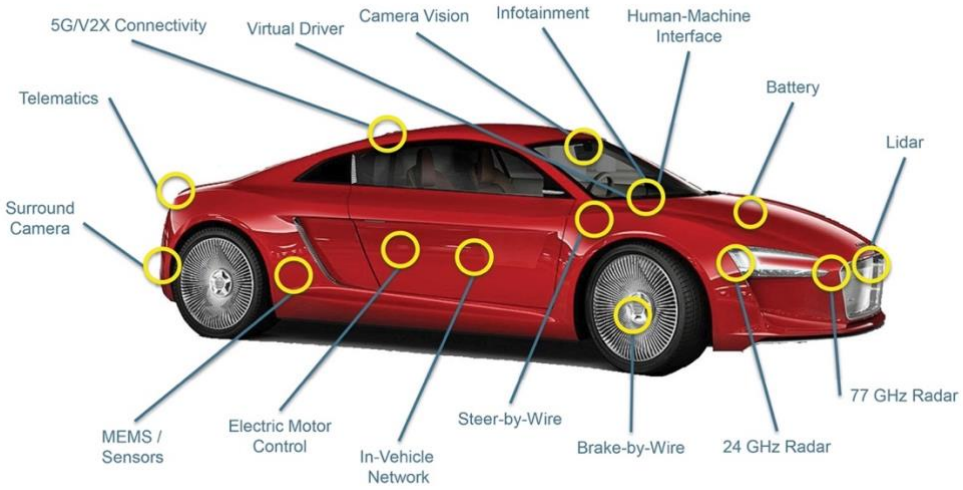

Fig. 2.4 Componenti principali di un veicolo

Ipoteticamente un veicolo potrebbe essere autonomo solo con l'utilizzo dei sensori, ma installare hardware come sensori e creare software ad hoc è troppo costoso per rendere accessibile il prezzo di acquisto di una macchina non di lusso.

Qui entra in gioco la comunicazione esterna, questa aiuta il sistema interno ottenendo informazioni che possano aiutarlo a vedere oltre il raggio dei propri sensori. Principalmente si occupa dei far connettere tra di loro i veicoli e le infrastrutture sfruttando una tecnologia chiamata VANET che sfrutta lo standard DSRC per la comunicazione a corto raggio mediante connessioni non cablata come il Wi-Fi e tecnologia LTE o 5G per le trasmissioni "Long Range".

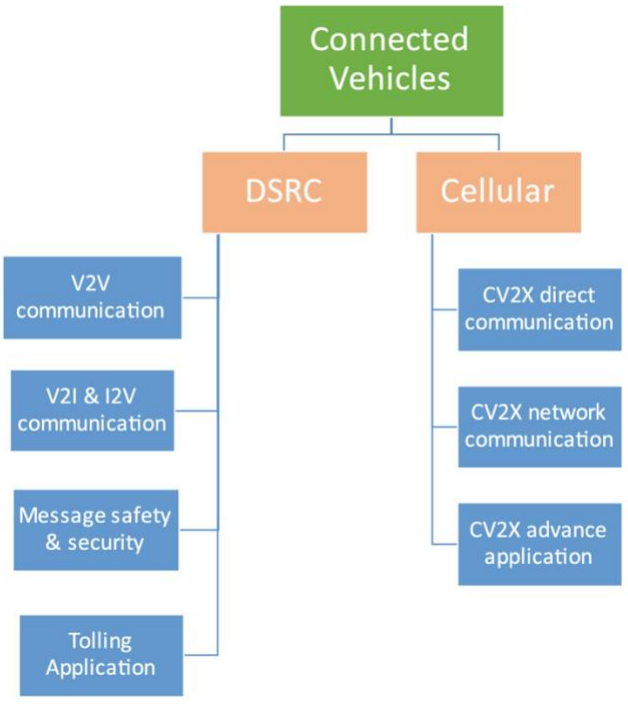

Fig. 2.5 Divisione VANET

3. Cybersecurity in IAV

Come già discusso in precedenza le minacce informatiche nel mondo Automotive stanno aumentando esponenzialmente a causa del sempre più consistente numero di veicoli e target da colpire, spesso e volentieri dotati di protezioni deboli, facilitando l'accesso a persone non autorizzate. Pertanto, la sicurezza informatica nei veicoli intelligenti e autonomi è una combinazione di sicurezza fisica, modellazione delle minacce, sicurezza delle informazioni, politiche, standard, legislazione e strategie di mitigazione del rischio. La Figura 3.1 illustra alcuni elementi dei IAV in termini di sicurezza fisica e informatica; in particolare, mostra le parti vulnerabili che vengono facilmente prese di mira dagli aggressori malintenzionati, i diversi mezzi diversi utilizzati e il loro impatto sulla sicurezza del veicolo [6].

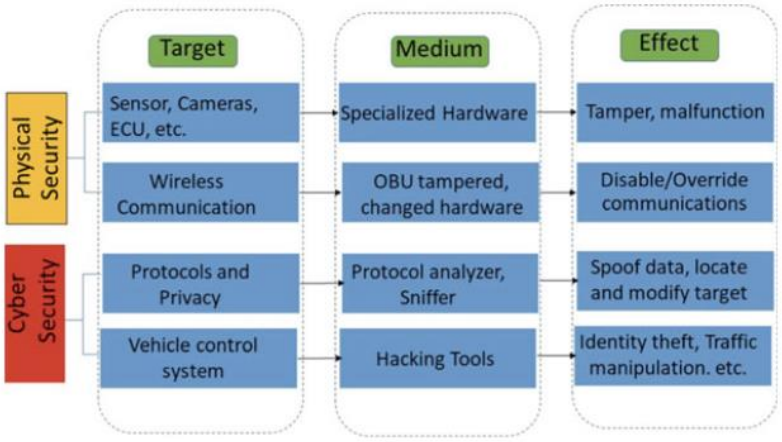

Fig. 3.1 Canali di attacco nel mondo Automotive

La protezione dai "cyber attack" consiste principalmente nell'adottare un'adeguata prevenzione installando sistemi di sicurezza che non l'ascino entrare l'intruso, ma nel caso falliscano e l'attacco riesce bisogna identificare il l'anomalia ed eliminarla prima che provochi conseguenze irreversibili che potrebbero violare la privacy o addirittura costare la vita del conducente. Gli elementi del veicolo devono essere protetti, in primis singolarmente, isolando diversi componenti in base alle loro funzioni, poi, proteggendo le loro interfacce, salvaguardando le reti all'interno del veicolo, e criptando i canali di comunicazione.

3.1 Cybersecurity Framework

Nel 2019, il National Standards and Technology Institute (NIST) ha lanciato la versione aggiornata 1.1 del Cyber Security Framework (CSF) per migliorare l'infrastruttura critica di sicurezza informatica e per aiutare le istituzioni nel loro percorso verso lo sviluppo di sistemi informatici sicuri (Figura 3.2).

Fig. 3.2 NIST Framework

Il framework è diviso in cinque fasi che coprono l'identificazione dei rischi e delle vulnerabilità, la protezione e la manutenzione delle infrastrutture critiche, il rilevamento dei rischi informatici, la risposta adeguata agli attacchi e il ripristino degli elementi coinvolti.

1. *Identificare:* è necessario identificare dati, apparecchiature, processi e risorse che riguardano l'impresa e che le permettono di svolgere le sue funzioni, analizzando le minacce da cui potrebbero essere colpiti, i pericoli che corrono e le vulnerabilità, effettuando in fine una valutazione del rischio e assegnando delle priorità.
2. *Proteggere:* dopo aver effettuato l'identificazione bisogna sviluppare e attuare una protezione adeguata a garantire la sicurezza del sistema dagli attacchi informatici. I dati devono essere acceduti solo da persone autorizzate mediante credenziali valide, inoltre non tutti possono effettuare tutte le operazioni sulle informazioni se no il rischio commettere errori è più alto. Insomma, è necessario attuare soluzioni di sicurezza strategiche per garantire la stabilità di tutti gli elementi dell'impresa.
3. *Rilevare:* questa fase si occupa dell'installare sistemi di monitoraggio e rilevamento in modo da cogliere comportamenti anomali prima che portino ad incidenti o malfunzionamenti con possibili conseguenze dannose. Questi sistemi

di controllo vengono mantenuti sempre in modo da garantire un rilevamento tempestivo ed efficace.

4. *Reagire:* dopo aver rilevato un evento estraneo si adottano procedure e meccanismi di sicurezza per contrastarlo, ovviamente più è accurata la fase di rilevamento più si sa contro che cosa si combatte, rendendo la fase di reazioni più efficace ed efficiente.
5. *Ripristinare:* nell'ultima fase, anche se si è riusciti ad eliminare la minaccia, questa può aver lasciato dei danni ad alcune risorse dell'impresa, di conseguenza è obbligatorio ripristinare questi elementi compromessi e ritornare alla piena capacità esecutiva.

Questo template può essere utilizzato in ogni attività ma, ovviamente, ogni campo ha sfide e minacce specifiche, diversi difetti e diverse tolleranze di pericoli, vari procedure e processi da seguire e rispettare.

3.2 Livelli di sicurezza in base alla progettazione

Per rendere un veicolo sicuro ed avere tecniche di protezione valide la cybersecurity deve essere considerata fin dall'inizio della progettazione e in tutte le fasi di sviluppo, cercare di includerla alla fine porta alla impossibilità di ridurre un gran numero di rischi, aumentando la vulnerabilità del mezzo.

Le strategie di attacco informatico sono in continuo sviluppo, quindi, è impossibile bloccarle tutte ad un livello di sicurezza, ciò implica la necessità di un monitoraggio continuo e la costruzione di un'architettura basata su livelli di protezione ognuno che filtra sempre di più le minacce rendendo riducendo agli aggressori la possibilità di successo in un attacco.

Esistono cinque livelli tecnologici per proteggere qualsiasi azienda o organizzazione, ovviamente se tutti e cinque sono stati analizzati e protetti a dovere:

1. *Perimetro:* lo strato perimetrale protegge le interfacce esterne, come un ancoraggio sicuro a prova di manomissione, che collega il veicolo al mondo esterno. L'obiettivo di questo livello è filtrare e controllare la connessione esterna dell'IAV limitando l'accesso al sistema e consentendolo solo a chi è davvero autorizzato a farlo.
2. *Rete:* in questo livello si utilizzano tecnologie che tutelano la relazione tra la rete esterna e quella interna, principalmente tramite utilizzo di firewall e gateway che permettono ai soli dispositivi legittimi di comunicare e interagire con i componenti del veicolo.
3. *Endpoint:* con endpoint si intendono tutti i dispositivi fisici che contiene l'autovettura, ognuno protetto singolarmente, specialmente con sistemi di monitoraggio e rilevazione di anomalie che possono presentarsi su di loro prevenendo intrusioni e garantendo che un messaggio inviato da un endpoint è autenticato ed integro trami algoritmi di cifratura.
4. *Applicazioni:* questo livello garantisce che i software in esecuzione sui vari dispositivi in particolare il processore sia legittimo e soprattutto affidabile, non possiamo mentre siamo alla guida avere un crash del sistema o magari malfunzionamenti a componenti necessarie alla guida.
5. *Dati:* il veicolo immagazzina, trasmette e utilizza una grande quantità di dati, molto spesso sensibili e privati; perciò, preservare la confidenzialità, integrità e disponibilità dei dati è fondamentale sia perché servono al IAV per svolgere le sue funzioni ma soprattutto perché un'impresa è obbligata a mantenere riservate le informazioni di tutti gli utenti.

4. Internet of Vehicles (IoV)

4.1 V2X

Lo scambio dei messaggi tra veicoli interconnessi si basa su VANET. A causa del progresso in questo settore si da sempre più importanza allo scambio di informazioni per migliorare la guida sicura, la situazione del flusso del traffico evitando congestione, ridurre il numero di incidenti e molto altro. L'obbiettivo principale delle autovetture connesse è migliorare la sicurezza stradale e ciò può essere ottenuto facendo comunicare un veicolo con ciò che lo circonda creando delle vere e proprie reti in movimento. Le connessioni a seconda dei due soggetti, tra i quali si instaurano, vengono divise in quattro categorie:

- *V2I (Vehicle-to-infrastructure):* comunicazione tra il veicolo e tutte le strutture che lo circondano con i quali scambiano informazioni, ovviamente interno al suo raggio di comunicazione.
- *V2N (Vehicle-to-network):* connessione con server remoti per sfruttare servizi basati su cloud collegandosi tramite rete cellulare al veicolo.
- *V2V (Vehicle-to-vehicle):* trasmissione con i veicoli nelle immediate vicinanze.
- *V2P (Vehicle-to-pedestrian):* stesse caratteristiche della connessione V2V però eseguita con gli elementi più vulnerabili sulla strada, ovvero i pedoni.

L'unione di queste tipologie forma il V2X, cioè il "vehicle-to-everything".

4.2 Ambiente IoV

Ormai Internet gioca un ruolo fondamentale nelle nostre giornate, senza non si potrebbe svolgere praticamente nessuna delle attività quotidiane, sia a livello personale sia lavorativo. Tutti traggono enormi benefici da esso, in particolare ci sono dispositivi elettronici che possono connettersi l'uno con l'altro, fornendosi servizi a vicenda

creando IoT (Internet of Things). Con il progresso dell'IoT ogni settore ha iniziato a ragionare al proprio ambiente, identificando necessità e difficoltà diverse fino a far nascere nel mondo dei veicoli l'IoV (Internet of Vehicles), ovvero una complessa rete veicolare connessa ad internet con vari sensori, varie tecnologie che raccolgono dati da tutto ovvero V2X.

Fig. 4.1 Internet of Vehicles

Le caratteristiche del IoV sono:

- *Comunicazione complessa:* la comunicazione in IoV si basa su diversi tipi di sensori interni ed esterni installati nei veicoli come LiDAR, radar, GPS, telecamere, sensori di parcheggio ecc.; tutti che sfruttano tecnologie e standard diversi ma che devono comunicare in modo sicuro. La complessità aumenta con il cambiamento della densità e della velocità dei veicoli, ad esempio negli scenari autostradali ci saranno meno veicoli e si muoveranno a una velocità molto elevata. Tuttavia, in uno scenario urbano, i veicoli si muoveranno a bassa velocità ma ci saranno interferenze da parte dei veicoli vicini. L'IoV è in grado di gestire la complessità della comunicazione nelle reti veicolari.
- *Alta scalabilità:* l'incremento di veicoli e informazioni che sono necessarie scambiare rendono il fattore della scalabilità essenziale. Quando si produce un

software o un componente bisogna essere sicuri che funzioni anche per grandi quantità, bisogna che si pensi anche al futuro.

- *Comunicazione localizzata:* ogni veicolo ottiene informazioni sempre nuove, non ci sono mai situazione identiche, perché pur essendo in una stessa località e le strutture che ti circondano sono le stesse, si modificano le comunicazioni V2V e V2P
- *Capacità energetica e di calcolo:* rispetto ai dispositivi IoT, i veicoli hanno una energia quasi illimitata essendo fornita di una enorme potenza grazie alla batteria ma devono sfruttarla per effettuare calcoli quasi istantanei senza commettere errori.

4.3 Architettura a livelli del IoV

Negli anni si è pensato a come creare una architettura nel mondo automotive per garantire flessibilità, scalabilità e sicurezza. Quando i veicoli hanno iniziato ad essere digitali si è pensato di strutturare a livelli le varie funzionalità e gestirle una alla volta per poi metterle in comunicazione. Partendo da architetture a due livelli si è arrivati fino ad oggi dove, con la presenza di veicoli intelligenti e autonomi, si è arrivati ad una struttura con sette livelli.

1. *Interfacce:* Il primo livello si occupa dell'interazione tra l'utente e i nodi veicolari. Il livello di interazione è responsabile della gestione delle notifiche ottenute da diverse interfacce come quella uditiva (come l'emissione di un segnale acustico/avviso), l'interfaccia visiva (come le luci tremolanti sul parabrezza) e l'interfaccia tattile (come le vibrazioni sul sedile). Gestisce anche le interfacce all'interno del veicolo, tra i veicoli e altre diverse interfacce oggetto.
2. *Acquisizione dati:* Il secondo livello è di acquisizione dei dati, raccoglie informazioni da diverse fonti come intra-veicolo, inter-veicolo, sensori, attuatori, RSU, semafori e altri dispositivi intelligenti che sono rilevanti per la sicurezza stradale, i dati sul traffico e l'infotainment. Poiché i veicoli stanno diventando sempre più intelligenti, vengono installati un gran numero di sensori

che generano enormi quantità di dati, rendendo complesso raccoglierli, mantenerli e diffonderli quasi in tempo reale.

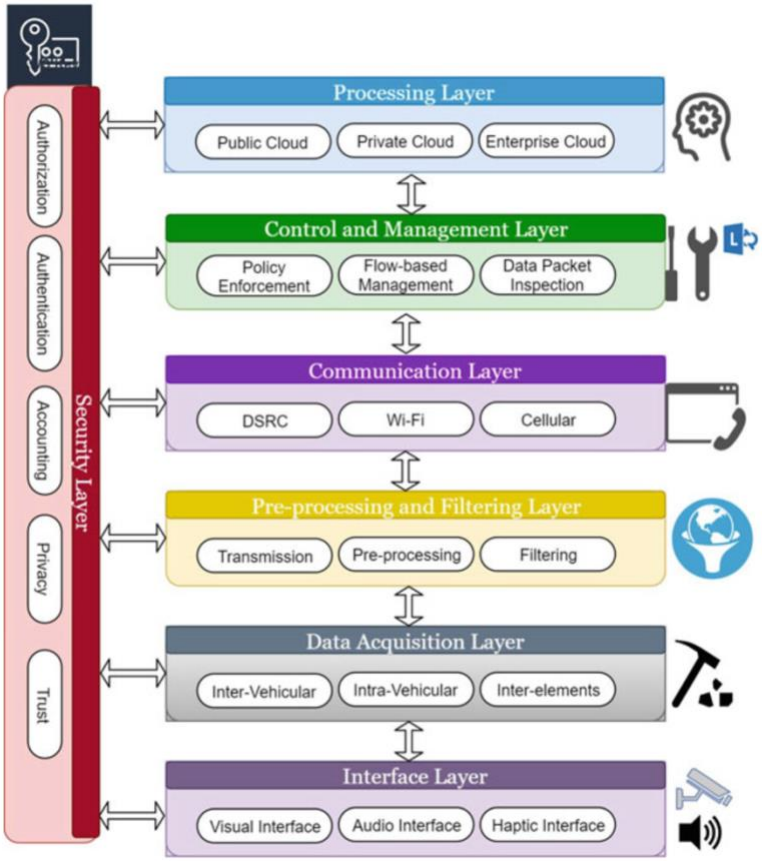

Fig. 4.2 Architettura a sette livelli

3. *Pre-elaborazione e filtraggio dei dati:* Avendo una gran quantità di dati da gestire, spesso e volentieri, contengono informazioni irrilevanti, da poter scartare. Avere un buon sistema di filtraggio limita la congestione di dati e il sovraccarico di trasmissioni e, considerando la necessità di una trasmissione veloce, effettuare già una selezione delle informazioni utili permette di risparmiare tempo e fatica.
4. *Comunicazione:* In IOV, ci sono diversi tipi di modalità di comunicazione veicolare eterogenea come 802.11p, Wi-Fi, reti cellulari, comunicazioni wireless a corto raggio. A seconda delle caratteristiche dell'ambiente di comunicazione, la rete fornisce connettività e servizi senza soluzione di continuità con QoS (Quality of Service) ottimali per gli utenti, il tutto dipende da vari parametri

come la tecnologia wireless disponibile, i requisiti di posizione e servizio dei veicoli. Questo livello fornisce una tecnica intelligente che seleziona la rete wireless più appropriata in base alle informazioni e alla misurazione appropriate per avere la miglior qualità di comunicazione.

5. *Gestione e controllo:* questo livello è responsabile del controllo delle informazioni, ispezionarle ed indirizzarle oltre a captare se ci sono informazioni anomale o incongruenti.
6. *Elaborazione:* dopo aver acquisito, filtrato, controllato e gestito i dati è il momento di elaborarli, il sesto livello si occupa di eseguire scelte intelligenti basate sull'analisi statistica, Machine Learning e altre tecniche, tutto in modo rapido ed accurato con meno errori possibili.
7. *Sicurezza:* L'ultimo livello è un livello verticale, perché si relaziona con tutti i livelli precedenti garantendo la sicurezza necessaria sia per prevenire attacchi dall'esterno che per evitare anomalie all'interno del veicolo, implementando meccanismi di autorizzazione, autenticazione, e molto altro, preservando confidenzialità, integrità e disponibilità dei dati.

4.4 Sfide in IoV

Un mondo così dinamico e così frenetico, sempre ricco di novità non deve far dimenticare le sfide presenti nel settore automotive e quali nuove sfide e difficoltà ogni giorno si presenteranno. Molte per il momento sono sotti controllo ma con l'aumentare del numero dei veicoli potrebbero tornare a causare problemi per questo non vanno dimenticate e devono sempre essere al centro dei pensieri di un softwarista.

- *Delay:* avendo bisogno di risposte immediate sappiamo che non può esserci un ritardo elevato tra la trasmissione di un pacchetto e la sua ricezione.
- *Mancanza di standard:* nel IoV vengono usati molti sistemi di comunicazione, non esistono standard unici rendendo così più difficile anche se possibile

integrare molti metodi di condivisione per lo scambio di informazioni ma senza una soluzione di continuità.

- *Connettività:* la connettività di rete è la spina dorsale del sistema, senza di questa è impossibile eseguire il 90% delle azioni in un veicolo oggi e purtroppo esistono ancora zone, come campagna o montagna dove la connettività è scarsa se non addirittura assente.
- *Tolleranza:* Il sistema IOV deve essere tollerante ai guasti e alla perdita di pacchetti in rete, dato che sappiamo che una rete completamente affidabile non esiste, al contrario è molto fragile.
- *Interoperabilità:* in questo mondo rientrano modelli di rete anche molto diversi tra loro e farli cooperare non è sempre una sfida facile, considerando anche il fattore della scalabilità dato che il numero di nodi veicolare è sempre maggiore.
- *Privacy e sicurezza:* questa come già detto rimane la sfida più difficile da affrontare, persone con cattive intenzioni cercano ogni giorno, milioni di tentavi al giorno, di impossessarsi di qualcosa che non gli appartiene. Un sistema non sicuro non può essere utilizzato nel IoV, troppo sensibile a violazioni sia per le aziende ma soprattutto per gli utenti.

5. Case Study

5.1 Digital Twin

Da qualche anno si è inserita nel mondo automotive l'idea e l'utilizzo del Digital Twin. Il Digital Twin, tradotto "gemello digitale", è un modello non fisico che è stato progettato per riflettere accuratamente un sistema artificiale o fisico, in cui i sensori sono posizionati per acquisire una varietà di dati relativi a diversi aspetti riguardanti le prestazioni del sistema. Questi dati vengono poi trasmessi a un sistema di acquisizione e applicati alla copia digitale. Quando la copia digitale viene aggiornata con i dati pertinenti, il modello virtuale può essere utilizzato per l'implementazione di varie simulazioni, che possono portare a potenziali miglioramenti, creando informazioni preziose, che possono quindi essere applicate al sistema esistente nel mondo fisico. Sebbene i gemelli digitali abbiano un grande potenziale, il loro uso non è una necessità per ogni prodotto fabbricato. Non tutti gli oggetti possono essere considerati abbastanza complicati da necessitare degli intensi e tattici sensori di flusso di dati richiesti dai gemelli digitali, né vale sempre la pena dal punto di vista finanziario investire risorse importanti per la creazione. Pertanto, i settori industriali che, ad oggi, impiegano questa tecnologia sono quelli che sviluppano e producono prodotti del settore di nicchia.
Integrare il Digital Twin aiuta principalmente in quattro funzioni del processo di vita di un determinato prodotto:

- *Design:* I processi di visualizzazione possono essere utilizzati durante la progettazione per la verifica e l'ispezione dell'intero assemblaggio del progetto 3D del prodotto al fine di verificare che la corrispondenza e l'adattamento siano quelli desiderati.
- *Diagnostica:* Le simulazioni insieme alle varie letture dei sensori possono analizzare alcuni dati non accessibili come varie forze e sollecitazioni applicate in diverse parti del prodotto.

- *Predizione:* Con algoritmi di intelligenza artificiale e deep learning, le previsioni possono essere condotte in modo accurato e tempestivo ai fini della longevità dell'apparecchiatura o dell'unità. Inoltre, tutte le informazioni sono disponibili in tempo reale e aiutano nella progettazione di piani di manutenzione razionali per la riduzione di potenziali interruzioni di funzionamento non programmate.
- *Manutenzione:* Un gemello digitale può analizzare i dati sulle prestazioni raccolti entro un determinato intervallo di tempo e in varie condizioni. L'analisi combinata fornisce le informazioni necessarie per gli utenti, al fine di procedere con le opportune azioni di manutenzione.

5.1.1 Digital Twin nel Automotive

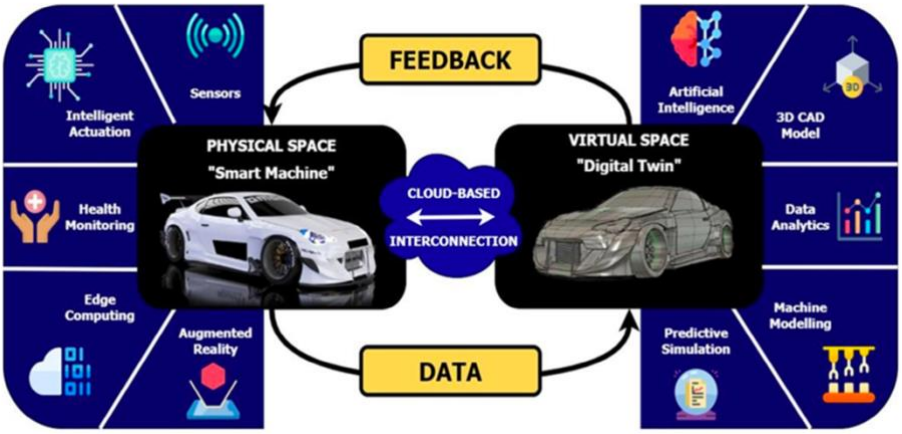

Fig. 5.1 Digital Twin nel settore automotive

L'integrazione del gemello digitale è ormai utilizzata anche nel mondo dei veicoli, la virtualizzazione in fase di progettazione unita all'infinità di sensori presenti e all'intelligenza artificiale rendono possibile effettuare delle simulazioni molto accurante. Nelle fasi iniziali dello sviluppo il Digital Twin è in grado di raccogliere le informazioni comportamentali del veicolo in termini di prestazione, fornendo dettagli preziosi ai progettisti; inoltre, con l'aumentare di componenti effettuare sempre dei test fisici sarebbe molto costoso in termini di tempo e denaro, perciò avere un gemello digitale simula l'intero sistema fornendo informazioni in termini di compatibilità,

interoperabilità e prestazioni, mettendo sotto stress il veicolo tramite condizioni di difficoltà per scoprirne i limiti e le debolezze, seguite dall'implementazione di correzioni e miglioramenti.

Oltre ad essere di grande aiuto nella fase di sviluppo, questa tecnologia vieni inserita nel veicolo e sfruttata durante tutta la sua vita specialmente per aiutare i meccanismi di Advanced Driver Assistance Systems. ADAS è la terminologia utilizzata per quanto riguarda i supplementi di sicurezza progettati per aumentare la sicurezza del conducente, dei passeggeri e dei pedoni riducendo al minimo il numero e la gravità degli incidenti automobilistici. Lo scopo di un ADAS è informare gli utenti quando vengono identificati potenziali pericoli imminenti, intervenire quando necessario affinché l'utente possa ottenere il controllo adeguato dell'automobile e prevenire incidenti o ridurre la gravità di un incidente quando potrebbe accadere. Questi meccanismi fanno molto affidamento sulla tecnologia Digital Twin perché utilizzano sensori che in combinazione con il cloud, in cui tutti i dati vengono archiviati e richiamati se necessario e con IA rilevano possibili minacce future o imminenti.

5.1.2 Case Study: rilevazione di un Cyber-attack

Per convalidare l'utilizzo di questa tecnologia nel mondo automotive, si è eseguito uno studio su come, sensori e radar, raccolgano dati utili al gemello digitale per identificare una anomalia dovuta ad un attacco informatico. La struttura di un flusso di dati mostrata da vari framework di analisi mette in evidenza il percorso dal quale si possono captare variazioni atipiche rispetto al comportamento naturale. Dopo aver rilevato il possibile attacco o malfunzionamento i sensori di monitoraggio possono essere programmati per attivare diverse contromisure per contrastare l'intruso, come richiamare alla guida il conducente, oppure disabilitare la funzionalità compromessa tutto per eliminare la

minaccia il prima possibile. Un attento caso di studio è stato effettuato sul sistema ACC (Adaptive Cruise Control), che si occupa di mantenere il veicolo ad una certa distanza dal veicolo precedente facendo accelerare o decelerare la vettura.

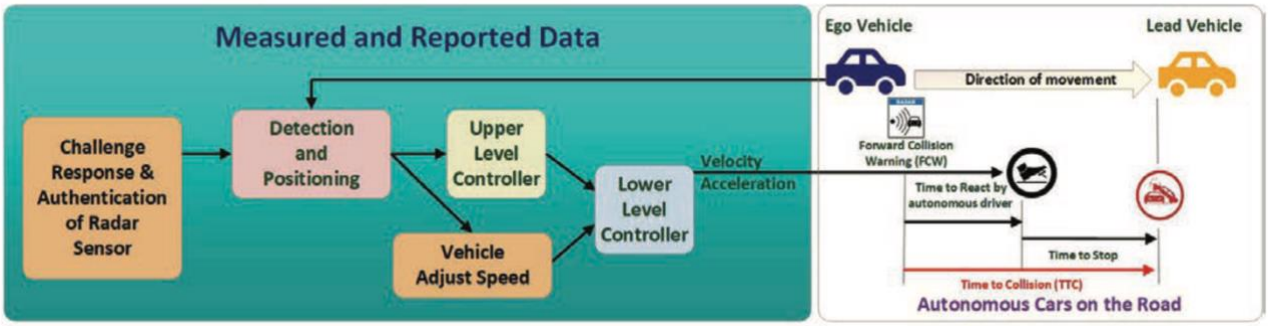

Fig. 5.2 Funzionalità Adaptive Cruise Control

La scelta del comportamento del veicolo è basta sui dati che i radar, principalmente quelli frontali dell'autovettura, mandano al sistema il quale li elabora e prende una decisione. Con la presenza di un Digital Twin tutte queste informazioni vengono mandate ad esso che incrociandole ed analizzandole con dati passati nel cloud, e con altri sensori presenti nel veicolo riesce a identificare se una fonte è compromessa, creando delle possibili simulazioni, anche in real-time.

Il vantaggio fornito dal gemello digitale per contrastare cyber-attacchi sta nel costruire modelli, implementati su di esso, predisposti per eseguire determinate azioni mediante un'analisi accurata dei dati ed algoritmi di IA, così da bloccare un attacco all'origine in modo da prevenire il problema e di non doverlo curare portando migliorie al mondo della guida autonoma, rendendola sempre più completa, priva di errori e di conseguenza più sicura.

Purtroppo, però esiste un grande limite utilizzando questo modello, ovvero il costo. Inserire componenti che effettuano rilevazioni precise e affidabili, e molto costoso, per non parlare della necessità di velocità di elaborazione dei dati per prendere decisioni immediate. In caso di Digital Twin questi componenti servirebbero per l'intero sistema ovvero per qualsiasi funzione della vettura, così facendo il costo per la produzione di tali prodotti renderebbe il mercato automobilistico quasi inaccessibile a molti utenti. Inoltre, un altro limite è la presenza di falsi positivi e negativi, si è in presenza di un

falso positivo quando un comportamento del Twin non corrisponde ad uno del sistema reale, ad esempio vulnerabilità restituite dallo scanning ma che in realtà non sono presenti in un modulo oppure alcune interazioni che in realtà non possono avvenire a livello hardware, invece c'è un falso negativo quando il modello non riproduce un comportamento che si verificherebbe nella realtà, possono sorgere vulnerabilità non ancora pubbliche o a componenti la cui presenza non è nota al gemello digitale.
Anche se, a mio avviso, quando si riuscirà a creare un modello di gemello digitale funzionante e privo di errori quasi al 100% si potrebbe iniziare ad abbattere i costi limitando o addirittura eliminando tutte le tipologie di test fisici ad oggi obbligatori perché vincolati da standard e normative internazionali.

5.2 TSC (Traffic Signal Controller)

Oltre ai veicoli, anche le città stanno diventando sempre più Smart. In questo caso di studio ci si sofferma sull'analizzare la comunicazione tra i veicoli ed uno degli elementi più presenti nelle strade ovvero i semafori. Da sempre ai semafori è collegato un controller che gli permette di cambiare il loro segnale dopo un certo intervallo di tempo per gestire gli incroci e cercando aumentare la transitabilità. Ormai da tempo i semafori, ovviamente, non sono impostanti sempre con le stesse tempistiche, bensì, si esegue un'analisi della posizione e delle necessità per trovare il miglior compromesso per ogni sistema. Con l'introduzione del IoV, come detto in precedenza, si ha la possibilità di scambiare informazioni da veicoli a qualsiasi dispositivo e viceversa; infatti, si è pensato di collegare al TSC dei dispositivi che possono captare i messaggi proveniente

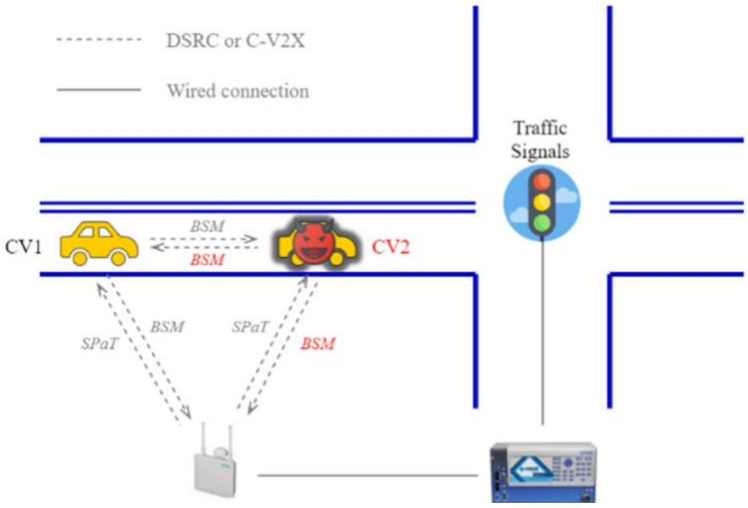

Fig. 5.3 Possibile minaccia

dalle automobili in modo da percepire se sta arrivando un'auto ad un semaforo, a che velocità e soprattutto se molte auto sono in attesa che il semaforo diventi verde. Tutto ciò, grazie alle tecniche di connessione moderne, rende perfino i semafori dei dispositivi intelligenti, in grado di prendere decisioni per evitare di congestionare il traffico. Purtroppo, però si sa che aggiungere dispositivi e tecnologie, aggiunge anche possibili vulnerabilità sfruttabili da hacker per scagliare attacchi verso il sistema.

5.2.1 Case Study: identificazione segnale compromesso

Si presenta un caso di studio sul controllo di un segnale da parte di un veicolo interconnesso.

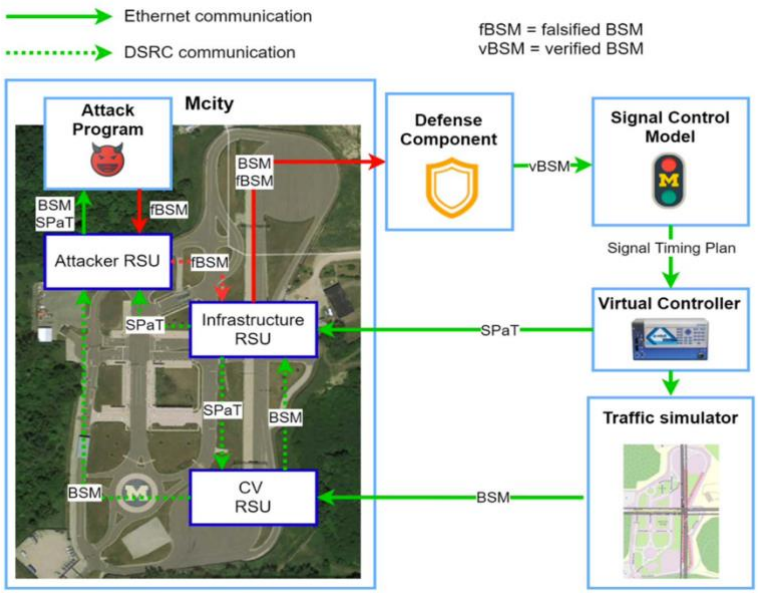

Fig. 5.4 Visione spazio del test

Innanzitutto, il semaforo è dotato di un router al quale vengono inviati segnali dai veicoli connessi, contenenti alcune informazioni rilevanti, principalmente posizione attuale e velocità. Tramite questi dati il TSC si occupa di calcolare la traiettoria delle vetture creando una sorta di tabella con la stima di tempo dell'arrivo al semaforo.
L'attacco utilizzato in questo caso consiste nel falsificare le informazioni di un veicolo modificandone così la risultante della sua traiettoria.

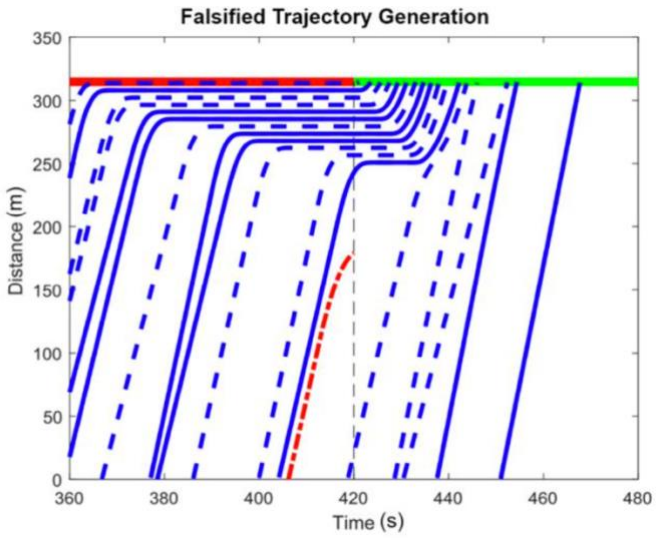

Fig. 5.5 Falsificazione traiettoria

Così facendo il semaforo, sfruttando un dato errato, prolunga la durata del verde inutilmente quando invece nessun veicolo è realmente in arrivo o addirittura, ipotizza che un veicolo si sia arrestato, creando una coda fantasma. Per evitare questo si presuppone un modello di difesa con l'obbiettivo di identificare la linea rossa in Fig. 5.5 (ovvero la traiettoria falsificata) per fare ciò si utilizza un framework che dopo essere stato "allenato" confronta le traiettorie l'una con l'altra utilizzando più dati e più precisi, come le distanze tra un veicolo e l'altro, così da cercare di identificare qualcosa di sospetto.

Questo modello di difesa, come mostrato in Fig 5.4, viene inserito subito prima dell'inserimento del segnale nel controller del semaforo così da rilevare anomalie e scartarle prima del processo decisionale per la scelta del tempo di attesa.

Dopo vari test si è arrivati alla conclusione che inserire un calcolo delle traiettorie con un modello di controllo e di conseguenza di difesa riesce a contrastare un attacco di un mal intenzionato, risulta comunque un incremento minimo nel delay come si osserva da Fig 5.6.

Scenario	PR	Attack goal	Experiment	Description	Average delay [s/veh]	Percentage Increase in Delay
1	100%	ETA = 64 s	1	Normal operation	39.50	-
			2	Attack w/o defense	48.58	23.0%
			3	Attack w/ defense	41.01	3.8%
2	50%	ETA = 64 s	4	Normal operation	43.38	-
			5	Attack w/o defense	51.03	17.6%
			6	Attack w/ defense	44.80	3.3%

Fig. 5.5 Risultati caso di studio

CONCLUSIONI

In conclusione, dopo aver approfondito l'ambiente in questione, si può evincere che il settore automotive sarà sempre più invaso da minacce informatiche ed essendo spesso in pericoli i diritti di privacy o la vita di un conducente sarà sempre più importante proteggersi. Inoltre, la tesi ha approfondito tecnologie che sono utilizzate oggi ma che ipoteticamente potrebbero evolversi, essere sostituite da alcune più innovative, o magari eliminate perché considerate non più utili. Il bello di questo mondo è che ci sarà sempre qualcosa di nuovo da scoprire o progettare, portando sempre più benefici a tutti i soggetti coinvolti.

Oltre ai meccanismi di sicurezza ed agli standard che devono essere sicuri è necessario però, sensibilizzare anche l'anello più debole della catena relativa alla sicurezza informatica, ovvero le persone. Si sottovaluta la formazione di quanto il web possa essere subdolo e pericoloso, ed un utente innocente si possa trasformare in una backdoor perfetta, sfruttata per intrufolarsi in un sistema al quale non si dovrebbe avere accesso. Sarà sempre più fondamentale evitare che involontariamente un dipendente dal punto di vista aziendale o un conducente dal punto di vista dei veicoli crei una vulnerabilità sfruttabile per recare danni in qualsiasi momento.

Per quanto riguarda la tecnologia del Digital Twin, ritengo che nei prossimi anni vedremo sviluppi sbalorditivi delle tecniche di Data Analisi, Intelligenza Artificiale e Machine Learning, questo renderà sempre più affidabile e sicuro il gemello digitale, che già oggi viene sempre più utilizzato nel Automotive, fino a farlo diventare uno standard in questo mercato.

Essendo un tema molto attuale, società, associazioni e stati stanno investendo molto nello sviluppo di nuove idee si a livello hardware che software; nel prossimo decennio sarà uno degli argomenti di maggior rilievo ed al quale serve dedicargli più risorse e tempo per poi magari sfruttare tutte le novità non solo in autovetture personali ma, magari, perfino in mezzi di trasporto pubblici.

BIBLIOGRAFIA E SITOGRAFIA

1. Kim, S., & Shrestha, R. (2020). Automotive cyber security. Springer Singapore. https://doi.org/10.1007/978-981-15-8053-6
2. R.D. Leighty, DARPA ALV (AutonomousLandVehicle) Summary (1986)
3. E.D. Dickmanns, V.Graefe, Dynamic monocular machine vision. Mach. Vis. Appl. 1(4), 223–240 (1988)
4. J. Shuttleworth, SAE Standards News: J3016 automated-driving graphic update (2019). [Online]. Available: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.
5. NIST, Framework for Improving Critical Infrastructure Cybersecurity V1.1 (2016).
6. G. De La Torre, P. Rad, K.K.R. Choo, Driverless vehicle security: Challenges and future research opportunities. Future Gener. Comput. Syst. (2018).
7. Piromalis, D., & Kantaros, A. (2022). Digital Twins in the Automotive Industry: The Road toward Physical-Digital Convergence. Applied System Innovation, 5(4), 65. https://doi.org/10.3390/asi5040065
8. Seshia, S. A., Hu, S., Li, W., & Zhu, Q. (2017). Design Automation of Cyber-Physical Systems: Challenges, Advances, and Opportunities. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 36(9), 1421–1434. https://doi.org/10.1109/tcad.2016.2633961
9. Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibanez, J. A. (2018). Internet of Vehicles: Architecture, Protocols, and Security. IEEE Internet of Things Journal, 5(5), 3701–3709. https://doi.org/10.1109/jiot.2017.2690902
10. J. Contreras-Castillo, S. Zeadally, J. A. Guerrero Ibáñez, A seven-layered model architecture for Internet of Vehicles. J. Inf. Telecommun. 1(1), 4–22 (2017)

11. A. Kumar, R.K. Mallik, R. Schober, A probabilistic approach to modeling users' network selection in the presence of heterogeneous wireless networks. IEEE Trans. Veh. Technol. 63(7), 3331–3341 (2014)
12. L.Xiao, W.Zhuang, S.Zhou, C.Chen, Learning based VANET Communication and Security Techniques (2019)
13. Brandi Sabino, Cyber risk e sicurezza informatica: un framework per la valutazione del sistema di sicurezza adottato da un'azienda IT, Università di Pisa (2015)
14. Feng, Y., Huang, S., Wong, W. Y., Chen, Q., Mao, Z. M., & Liu, H. X. (2022). On the Cybersecurity of Traffic Signal Control System with Connected Vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(9), 16267–16279. https://doi.org/10.1109/tits.2022.3149449
15. Marksteiner, S., Bronfman, S., Wolf, M., & Lazebnik, E. (2021). Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing. ArXiv (Cornell University). https://doi.org/10.1109/eurospw54576.2021.00020