CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

MACS

Multibrand Automotive Cybersecurity System

Cybersec veicolare IoT, con telemetria e SIEM in cloud

Ing. Marco Guardigli
direttore Tecnico TomWare,
mgua@tomware.it

TomWare

W3MAKE.IT

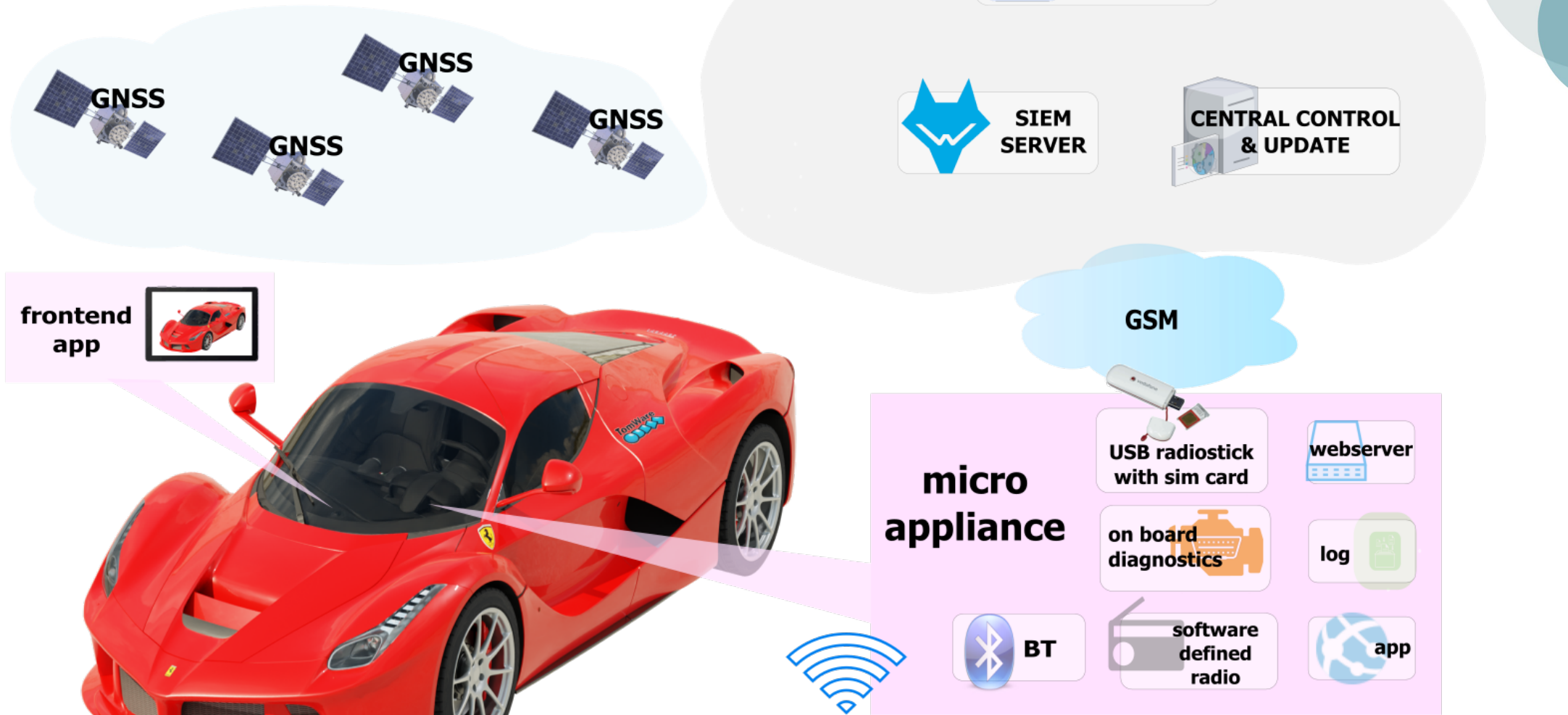
NETGATE

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Progetto MACS

1. Contesto
2. Obiettivi
3. Progettazione
4. Metodi
5. Realizzazione
6. Ulteriori sviluppi
7. Conclusioni

MACS:
Multibrand Automotive Cybersecurity System



CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Contesto

- Veicoli permanentemente connessi: link di veicolo e passeggeri
- 45% del costo di un veicolo è software†
- Funzioni: da HW dedicato a Software Defined (SD_*)
- Rischi sicurezza comunicazioni utenti ed ECUs (Electronic Control Units)
- Rari e costosi updates
- Cybersecurity molto attenzionata nel comparto automotive
- Un veicolo è un array di sensori mobile. Digitalizzazione e telemetria pervasive: raccolta dati da veicolo e da ambiente (situazioni, comportamenti, contesti, ...)

† *https://www.eetimes.com/projections-for-rising-auto-software-cost-for-carmakers/*

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Obiettivi

- Selezione e sviluppo tools per sicurezza automotive mutuati da contesti ICT (crossbreeding)
- Rilevamento e gestione proattiva eventi, con marcata indipendenza dai brand
- Progettazione di **centralina veicolare** per gestire i principali aspetti della sicurezza dei veicoli, sulla base dei risultati ottenuti nella sperimentazione di tecnologie ICT (informatica e telecomunicazioni),
- Prototipo basato sul modello, atto a dimostrare le soluzioni applicate ed i risultati ottenuti

- Timeframe Progetto: 1 dicembre 2021 .. 30 novembre 2023

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Progettazione

Architettura composta da una scheda a microprocessore ARM, caratterizzata da:

- MicroAppliance open source, linux based, brand independent
- Wireless link con Automotive Control Unit(s), compliance J1939+, diagnostiche std (ELM32*)
- Wireless link con dashboard mobile device: feed immagini, dati inerziali (accelerometri, gyros), magnetometro, GPS
- 4G/5G Wireless link, VPN con cloud services, WiFi di bordo
- Sensori SDR (Software Defined Radio) per rilevare eventi e attacchi RF sul territorio (con notifiche geolocalizzate ad autorità)
- Servizi RF identity management (RF fingerprinting, beacons, rfid tags)
- Cloud data collection (async), Event Correlation, Reporting + Alerting (da SIEM)
- Cloud based context based media streaming
- Cloud rendered contextual vehicle dashboard

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Metodi

In termini tecnici abbiamo lavorato sui seguenti aspetti:

- Integrazione microappliance con elettronica veicolare e sensoristica locale
- Acquisizione dati, filtering e buffering
- Comunicazioni asincrone cifrate con cloud data collector
- Aggiornamento/distribuzione parametrizzazioni alle microappliance
- Protocol Logging/Analysis/Dissection (+reverse engineering) in cloud
- Event detection e logging
- Dashboarding
- Alerting

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Realizzazione

- Micro-appliance di bordo versatile e standardizzata, brand independent, collegata via simcard a servizio cloud sviluppato appositamente per il progetto, con flussi multipli, gestione centralizzata, parametrizzazione dinamica
- Software di monitoraggio e raccolta dati raccoglie dati da sensori e bus veicolari, senza impattare le certificazioni dei preesistenti sistemi di elettronica veicolare E/E (Electric/Electronic)
- Raccolta dati su condizioni di filtraggio dinamiche e context-dependent, configurabili da remoto
- I dati trasmessi in forma cifrata sono raccolti su servizio cloud. Qui attività di analisi real-time SIEM (Security Information and Event Management) potranno rilevare anomalie, generando eventi, interpretazioni situazionali, con notifiche e allarmi a intestatari, manutentori o a specifici servizi di supporto
- Compliancy, privacy, normative e autorizzazioni dipendenti da utenti, geografia e contesto

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Componenti e fasi di lavoro

1. Integrazione e ingegneria microappliance prototipale
2. Modello architetturale dialoghi e protocolli
3. Interconnect locale ECU
4. Wifi + Bluetooth locale
5. SDR data collection con signal processing locale (digital filter)
6. Cloud based vpn server
7. Cloud based telemetry server
8. Cloud based contex sensitive interface rendering prototype
9. Cloud based SIEM
10. Cloud based system management
11. Cloud based alerting

Stato avanzamento 1/4

Ingegneria prototipo micro-appliance

Prototipo realizzato su piattaforma Raspberry PI v4. Si stanno quindi esplorando alternative basate su altri SOC (System On Chip), tra cui Raspberry PI Zero (https://www.farnell.com/datasheets/3587024.pdf) e Udoo Key (https://www.udoo.org/udoo-key/).

Sviluppo modello architetturale dialoghi e protocolli

Le componenti cloud faranno affidamento anche su componenti containerizzati. Si è deciso di affiancare agli strumenti IDE Visual Studio Code di Microsoft anche l'ambiente Neovim (https://www.neovim.io), corredato da una serie di plugin.

Interconnect locale ECU

Ci siamo basati su dispositivi che remotizzano e unificano le varie interfacce digitali presenti sulla porta diagnostica OBD2, utilizzando il "classico" chip ELM327, molto disponibile sul mercato da vari fornitori, che lo integrano in dispositivi di interconnect popolari, corredandolo con interfaccia bluetooth. Pressochè tutti i veicoli al momento espongono l'interfaccia CAN ISO 15765 per cui il chip 327, nella sua corrente disponibilità è perfettamente adeguato.

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Stato avanzamento 2/4

Wifi + Bluetooth locale

l sistema prototipale è stabile e funzionale come access point locale e si dimostra adeguato per servire in modo concorrente gli utenti del veicolo e il dispositivo dashboard/tablet di assistenza alla guida. Abbiamo sviluppato il codice per l'acquisizione dei dati inerziali, giroscopici e accelerometrici, e abbiamo sviluppato funzioni di acquisizione fotografica dalla telecamera, non inizialmente previste.

SDR data collection con signal processing locale (digital filter)

Le componenti software per l'analisi dei campioni provenienti dalla SDR (Software Defined Radio) si sono dimostrate complesse e hanno spiccate dipendenze da librerie soggette a frequenti aggiornamenti. Abbiamo realizzato un servizio di raccolta dati, in grado di ascoltare sulle adeguate bande di frequenza, e un sistema di digital filtering preliminare. Si effettuano campionamenti di breve durata, da spedire al cloud per analisi successive offline. A seguito di numerose disclosure di strumenti di attacco (rolljam) a sistemi a rolling code comunemente in uso, abbiamo osservato una forte attenzione alle tematiche di sicurezza sulle componenti a radiofrequenza. Sono inoltre emersi dispositivi e relativi software estremamente accessibili per attacchi su dispositivi RF (evilcrow e flipper: https://github.com/joelsernamoreno/EvilCrowRF-V2 e https://flipperzero.one/).

Cloud based vpn server

Realizzato con impiego delle tecnologie SSL-VPN, robuste, affidabili e ragionevolmente sicure. Segnaliamo che le recenti disclosure di problemi di sicurezza (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25136) che hanno impattato questi protocolli sono rilevanti solamente per le implementazioni più recenti ed avanzate, che sono moderne e meno robuste, e devono ancora essere adottate dall'industria. Nei nostri sistemi prototipali utilizziamo versioni precedenti più stabili non affette dal problema.

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Stato avanzamento 3/4

Cloud based telemetry server

Realizzato tramite un sistema di raccolta telemetrie basato su zabbix (www.zabbix.org). Zabbix è un rodato sistema di raccolta telemetrie e serie storiche, molto versatile per ambienti ICT, e per dati strutturati, tipicamente numerici. Su questi dati si possono fare analisi, ed è possibile effettuare rilevazione e generazione eventi all'attraversamento di thresholds definite anche in modo parametrico.

Cloud based contex sensitive interface rendering prototype

Si basa su un articolato sistema di scripts Python e su un relativo webserver CGI compliant, che può essere beseguito sia su windows che su linux. Nella nostra architettura il rendering è affidato ad una installazione di Blender (www.blender.org) su una workstation Windows, corredata con una scheda GPU Nvidia Quadro. La parametrizzazione consente di generare immagini su contesti diversi di ambientazione geografica e climatica (condizioni meteo sole/pioggia/nuvole/nebbia).

Cloud based SIEM

Per queste funzionalità ci basiamo sull'ambiente Wazuh (https://wazuh.com/) che è un ambiente SIEM open source. Wazuh è corredato di potenti funzionalità di analisi, e complementa il sistema di telemetria zabbix per tutte le necessità di correlazione e log aggregation (Wazuh raccoglie tipicamente i log da vari ambienti eterogenei distribuiti).

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Stato avanzamento 4/4

Cloud based system management

Composto da un sistema centrale che consente la distribuzione di comandi ed aggiornamenti ai microcontroller distribuiti, e che si basa sulle funzioni di remote execution di ssh, ed è agentless. Il sistema raccoglie centralmente e periodicamente l'esito di una serie di comandi eseguiti su ogni postazione remota. I dati raccolti sono archiviati in due distinte forme: su file system e su RDBMS.

Cloud based alerting

Sistema di notifica delle diagnostiche e degli eventi generati dai vari sottosistemi implementata con l'utilizzo dei classici protocolli email, per garantire la massima portabilità e funzionalità. Si integra con il motore di ticketing aziendale, che consente il tracking delle chiamate, la protocollazione e l'erogazione relativa dei servizi di supporto, con il tracking delle attività svolte in risposta.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Ulteriori sviluppi

- Interferenze RF
- RF digital filter, antenna design
- Riduzione consume, auto-standby/idling e power management
- Reliable wireless link with vehicle ECU (e architettura software avanzata: d-bus)
- RF based identity management (per funzioni di bluetooth and wifi anonymization in graduale e progressiva diffusione)
- Packaging e compliancy dell'hardware veicolare (ci attendiamo migliorie in fase di industrializzazione dei component, tramite sviluppo di una board dedicate). Riduzione cavi
- Stabilità/affidabilità
- Integrazione di tutti i moduli software in un aggregato coerente

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Conclusioni

- I veicoli sono sempre più a computer con le ruote
  (car computing=powerful mobile computing)
- Reti wireless: internet ovunque. Raggiungibilità e accesso: croce e delizia
- Cybersec ripete la sua storia: telefonia, mainframe, ict dipartimentale, PC, reti locali internet, dispositivi mobili, IoT e veicoli (anche errori si ripetono)
- Edge computing, hypervisor distribuiti: datacenter nelle antenne
- What next:
  - Parametrizzazione, personalizzazione e identità: cambio auto e parametrizzazione resta Identità e IoT abilitano molti nuovi servizi
  - Continuous integration & delivery (versionless)
  - Assistenti virtuali, modelli neurali alimentati da dati raccolti sulle strade.
    Sistemi edge based a bassa latenza

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Sottosistema cloud context rendering

- Interfaccia veicolare situazionale e contestualizzata
- Dati raccolti dal veicolo, contesto, configurazioni e dati storici contribuiscono a generare, da cloud, le visualizzazioni più adeguate
- Le telemetrie hanno fonti dati multiple
- open standard per dialoghi sw-sw (4 ambienti/ 6 linguaggi)