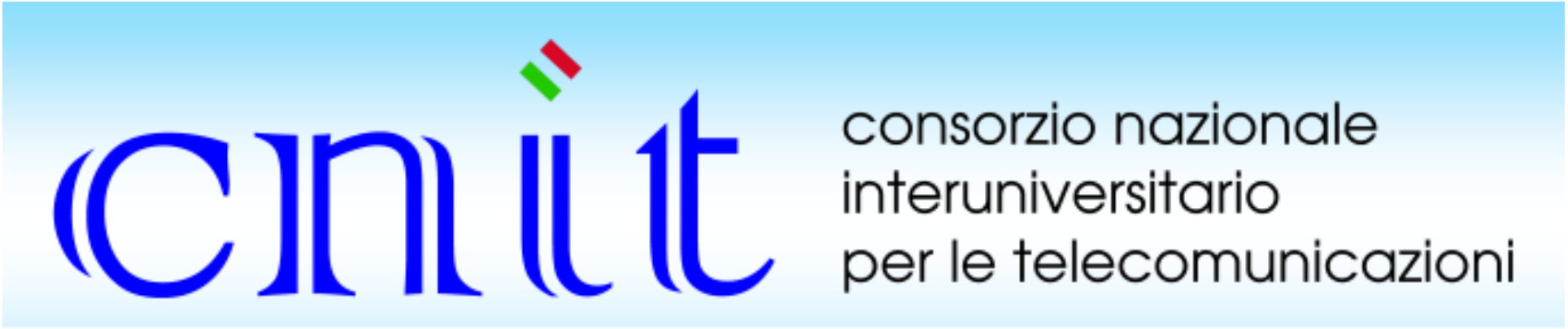


INCONTRO RINA/D'APPOLONIA-CNIT

TEMA 4: Security, inclusa Cybersecurity

Franco Davoli
franco.davoli@cnit.it

UdR CNIT di Genova e **Laboratorio Nazionale CNIT di** ***Smart, Sustainable and Secure Internet Technologies and Infrastructures, Genova***

consorzio nazionale interuniversitario per le telecomunicazioni

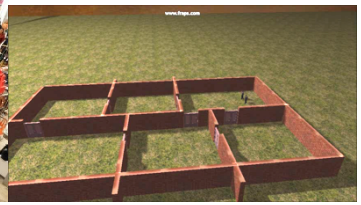
Ambito *Safety/Intelligence*

- Sistemi dinamici cognitivi
- Elaborazione di segnali multi-sensoriali per sorveglianza
- *Software* e *Cognitive Radio*
- Valutazione Bayesiana di oggetti e situazioni (*Bayesian Object and Situation Assessment*)
- Ambienti interattivi e cognitivi

Progetti europei (ARTEMIS) e progetti con aziende (Telecom, SelexES, …)

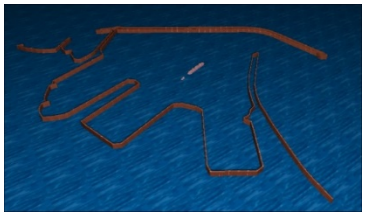
Cognitive Dynamic Systems

Cognitive crowd analysis



Bayesian Object and Situation assessment

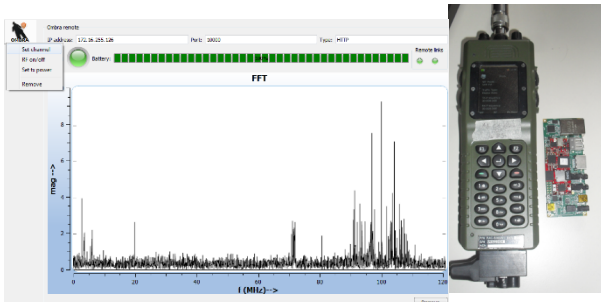
Activity Recognition and Abnormality Detection In Safety and Surveillance Applications



Routine behaviours can be defined by domain experts, simulation or learned from data

Software and Cognitive Radio

Spectrum Intelligence for jamming mitigation

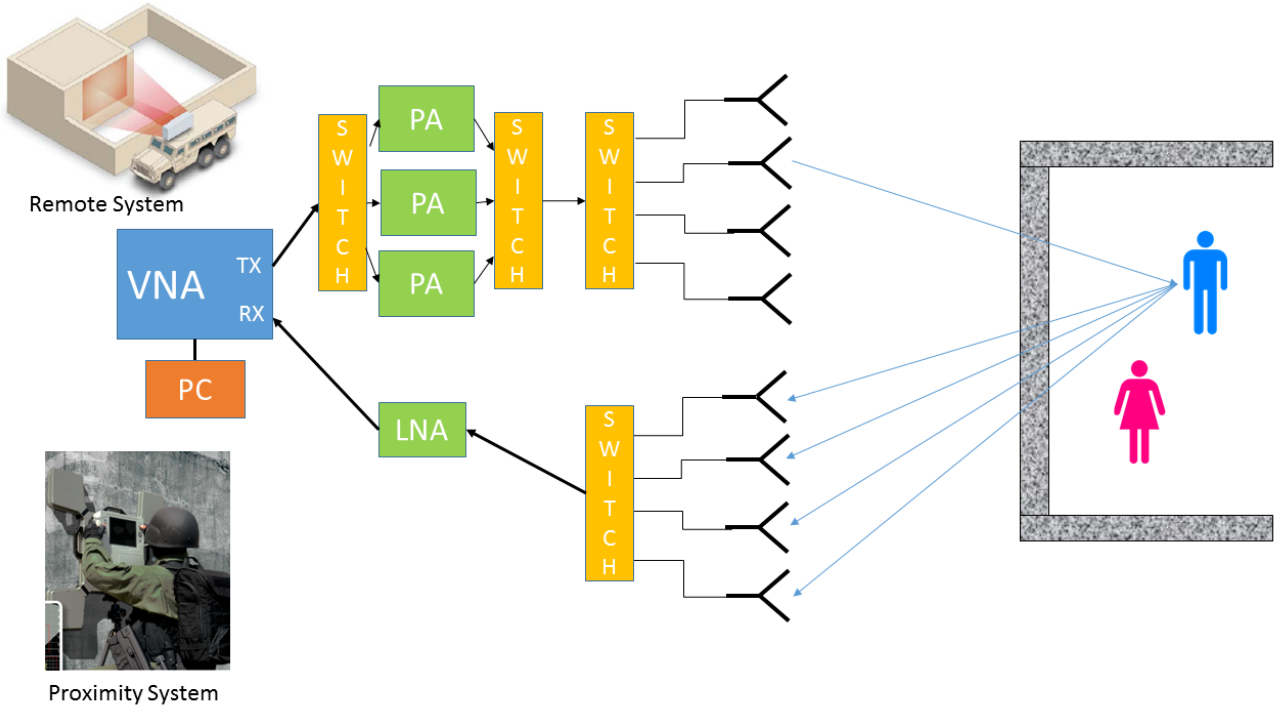


Text Mining* e *Semantic Analysis* per *Cyber Intelligence

- Metodi per *Preventive Cyber Security*
- *Early threat detection* da *Open Sources*
- Tecnologie di *Text Mining* per *Open Source INTelligence* (OSINT)
- Tecnologie di *Sentiment Analysis* per *profiling*
- Tecnologie di *Intelligence* da fonti *Social* (S/N e *blog*)

Collaborazioni con Aziende e Forze dell'Ordine

Attività: sviluppo di sistemi elettromagnetici innovativi di tipo *through-the-wall radar imaging*



Progetti attivi: Progetto PRIN 2015 (UniGE, UniCAL, UniRoma3, UniRoma1)

”U-VIEW (Ultra-wideband Virtual Imaging Extra Wall for high-penetration high quality imagery of enclosed structures)”

consorzio nazionale interuniversitario per le telecomunicazioni

Ambito *Cybersecurity*
Livello fisico

Physical-layer Security

Cos'è la *Physical-layer Security*?
Un insieme di mecccanismi che sfruttano le proprietà del livello fisico per rendere più difficoltoso un attacco

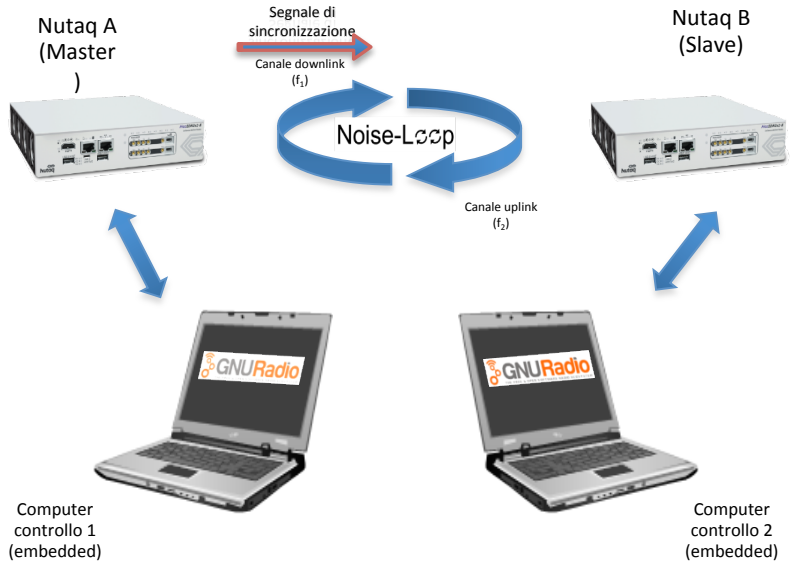
- *Noise-Loop Modulation*
- *Physical layer security* per sistemi *wireless*, con particolare esperienza per la generazioni di chiavi e l'autenticazione

Noise-Loop Modulation

Cos'è la *Noise-Loop Modulation*?
Lo sfruttamento della casualità intrinseca ai canali rumorosi per fornire un ulteriore livello di protezione

Cos'è il *quid novi* di questo metodo?
L'informazione di entrambe le sorgenti è contemporaneamente modulata con rumore. La violazione del meccanismo è matematicamente impossibile

Progetti:
1. **WiSEC, Ministero della Difesa, 2011-2016**
2. **iPhySec, sottoposto a ONRG (*Office of Naval Research Grant*), 2016**
3. **Progetto FIRB "Enhancing communication security by cross-layer physical and data-link techniques"**



Il sistema è stato realizzato e tutte le caratteristiche teoriche sono state dimostrate

Cifratura biometrica
(*Biometric encryption*)

- Estrazione di un «segno» dal corpo (impronta digitale, retina, voce, DNA, ecc.)
- Il segno è elaborato numericamente e se ne estrae una chiave di cifratura
- La chiave può essere applicata per:
  - Cifratura (Forte)
  - Autenticazione (del corpo)

Multimedia forensics

- Il dispositivo di acquisizione lascia tracce specifiche nelle immagini e nel video, dovute alle sue caratteristiche intrinseche
- Tali tracce possono essere studiate per capire se un contenuto visuale è stato manipolato, e per identificare il dispositivo che lo ha generato

Progetti: FENCE, DARPA, 2014-2018
Proposte progettuali: Biologin, H2020 FET, Sept. 2016

Sviluppo di tecniche e strumenti automatici per l'analisi dei sistemi "security-critical"

- Storie di Successo: indentificate vulnerabilità in
  - Single Sing-On for Google Apps
    - *Man-in-the-middle attack* nel protocollo di autenticazione usato da Google per il SSO delle Google Apps (utilizzato da 5ML di aziende nel mondo).
  - SAML Single Sign-On v.2.0 standard
    - Identificata violazione alla proprietà fondamentale dello standard SAML per il SSO.
    - La scoperta ha indotto OASIS a pubblicare Errata Corrige.
  - Android OS
    - Identificata vulnerabilità in Android che consente di realizzare un "fork-bomb attack" sui dispositivi.
    - Se sfruttato da malintenzionati avrebbe potuto portare ad attacco di *Denial-of-Service* su vasta scala. *Patch* proposta introdotta nelle ultime versioni di Android.
  - *Protocol for Strong Authen*tication (*multi-factor and multi-channel*)
    - Modellazione formale e analisi della sicurezza di soluzioni per l'Autenticazione Forte
  - NATO High-Assurance Automated Guard
    - Obiettivo: condivisione di informazioni importanti per una missione NATO tra partner (inclusi civili, ad es. Croce Rossa) - Definito modello e linguaggio per il controllo degli accessi - Sviluppati prototipi per l'analisi delle politiche di autorizzazione e per la loro applicazione (*enforcement*)

consorzio nazionale interuniversitario per le telecomunicazioni

Ambito *Cybersecurity* – Sicurezza Informatica

Progetti

- European Industrial Doctorate on "*Security & Trust of Next Generation of Enterprise Information Systems*", www.secentis.eu, in partnership with SAP, Marie-Curie Action
- *Automated Validation of Trust and Security of Service-oriented Architectures* (www.avanstssar.eu), FP7
- *Security Horizons*, PRIN Project, MIUR
- *FilieraSicura: Cybersecurity for the supply Chain*, funded by CISCO

consorzio nazionale interuniversitario per le telecomunicazioni

Gestione dell'identità digitale: Scenario Mobile

Obiettivi:

- Nuove soluzioni per la gestione delle identità digitali (autenticazione-autorizzazione) sui dispositivi mobili
- Conformità alle normative sulla gestione dell'identità digitale (SPID, eiDAS) e sulla *privacy*
- Supporto di diversi livelli di autenticazione (autenticazione a più fattori)
- Implementazione di riferimento *open source*

Scenario e-Health

trec cartella clinica del cittadino

Piattaforma di servizi che supporta **dottori** e **pazienti** nella gestione dei *Personal Health Records*

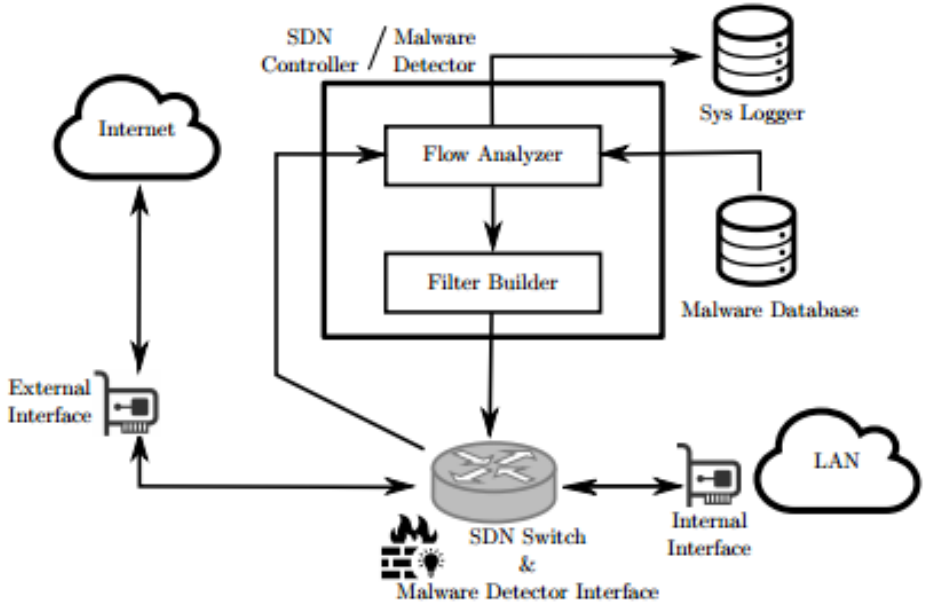
Soluzione innovativa che consente agli utenti di autorizzare in sicurezza *third party apps* ad accedere alla propria cartella clinica.

Sviluppo di una soluzione che garantisca:

- Autenticazione Forte dell'utente da piattaforma *mobile*
- Gestione dell'identità in rapporto con App sviluppate da terze parti
- Erogazione di un servizio di Single-Sign-On in ambito *mobile*

- *Statistical Analysis Based Intrusion Detection Systems* e SDN

	Deep Packet Inspection MD	Statistical Analysis Based AD
Processing method	It examines the whole packet content, analysing data at application layer looking for signatures/rules	It opens packet headers (e.g. at the IP and TCP/UDP layers) to identify flows and examines traffic statistically
Complexity	High	Low
Speed	Slow	Fast
Limitations	It cannot detect new virus or encrypted flow	A training data set is involved



- *Cyber Security, Business Continuity* e Robustezza di Reti Elettriche

Security monitoring / intrusion detection

- Tecnologie di sonde di rete
- Algoritmi per analisi traffico in *stream mode* (*real time, on the fly*) e per *complex event processing*
- Firme "comportamentali" per minacce multi-stage che superino i limiti delle firme tradizionali *rule-based*
- Applicazione a scenari avanzati di APT (*Advanced Persistent Threat*) e *lateral movement detection*
- *Deep Packet Inspection* (anche hardware).

Progetti EU FP7 PRISM, EU FP7 DEMONS, entrambi su tecnologie di monitoring.

Infrastrutture critiche (ICS) e sistemi SCADA

- Tecniche di monitoraggio adattate a sistemi e protocolli SCADA
- *Security information and event management* (SIEM) per correlazione eventi su infrastrutture critiche
- *Vulnerability assessment* e *penetration testing* per sistemi SCADA.

Progetto H2020-SCISSOR, *Security in Smart Grids*, Architettura di *security monitoring* per sistema SCADA della Società Energia Favignana (sull'isola).

Controllo di accesso Attribute Based (ABAC)

- Tecniche di controllo di accesso basate su attributi (piuttosto che su ruoli) – di forte interesse NIST dal 2013
- Integrazione con tecniche crittografiche (*Attribute Based Encryption*)
- Applicazione ABAC a scenari IoT

Progetto H2020-RECRED, su *access control e identity management* nella *call Digital Security*; progetto H2020-SYMBIOTE per la parte IoT

Altre attività

- *RFID security* e relativi attacchi (*wormhole attack* ai sistemi di pagamento *Near Field Communication* – NFC)
- Sicurezza in SDN
- Tecniche per la *privacy* e *business confidentiality*, tra cui tecniche crittografiche per *data sharing* e *secure multiparty computation* tra domini eterogenei.
- Sviluppo di protocolli per sicurezza ed integrazione di algoritmi proprietari in protocolli esistenti (integrazione di soluzioni proprietarie in *Transport Layer Security* – TLS).
- Sistemi di raccomandazione (ed in parte anche sistemi di reputazione)
- Ingegnerizzazione e programmazione di *malware* polimorfi

- Autenticazione per sistemi di navigazione satellitari

  Progetto ESA su autenticazione per sistemi di navigazione satellitare globali (GNSS, Galileo); Attività per la Commissione Europea (collab. Quascom, GMV) su autenticazione SBAS (EGNOS); Progetto per ESA (collaborazione Quascom, CGI) su *key management* per GNSS

consorzio nazionale
interuniversitario
per le telecomunicazioni

UdR CNIT coinvolte

- UdR di Genova e Laboratorio Nazionale CNIT di *Smart, Sustainable and Secure Internet Technologies and Infrastructures,* Genova
  - Prof. Franco Davoli, Prof. Alessandro Armando, Prof. Mario Marchese, Prof. Matteo Pastorino, Prof. Carlo Regazzoni, Prof. Rodolfo Zunino (nome.cognome@unige.it)
- UdR di Firenze
  - Prof. Enrico Del Re (enrico.delre@unifi.it), Dr. Lorenzo Mucchi (lorenzo.mucchi@unifi.it)
- UdR di Roma Tor Vergata
  - Prof. Giuseppe Bianchi (giuseppe.bianchi@uniroma2.it)
- UdR di Bari (collabora con Roma 2)
- UdR di Padova
  - Prof. Stefano Tomasin (tomasin@dei.unipd.it)
- UdR Università della Calabria
  - Prof. Sandra Costanzo (costanzo@deis.unical.it)
- UdR Roma3
  - Prof. Giuseppe Schettini (giuseppe.schettini@uniroma3.it)
- UdR Roma La Sapienza
  - Prof. Renato Cicchetti (cicchetti@diet.uniroma1.it)